

DIN EN 61069-5



ICS 25.040.40; 35.240.50

Ersatz für
DIN EN 61069-5:1995-09
Siehe Anwendungsbeginn

**Leittechnik für industrielle Prozesse –
Ermittlung der Systemeigenschaften zum Zweck der
Eignungsbeurteilung eines Systems –
Teil 5: Eignungsbeurteilung der Systemverlässlichkeit
(IEC 61069-5:2016);
Deutsche Fassung EN 61069-5:2016**

Industrial-process measurement, control and automation –
Evaluation of system properties for the purpose of system assessment –
Part 5: Assessment of system dependability
(IEC 61069-5:2016);
German version EN 61069-5:2016

Mesure, commande et automation dans les processus industriels –
Appréciation des propriétés d'un système en vue de son évaluation –
Partie 5: Evaluation de la sûreté de fonctionnement d'un système
(IEC 61069-5:2016);
Version allemande EN 61069-5:2016

Gesamtumfang 38 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE

Anwendungsbeginn

Anwendungsbeginn für die von CENELEC am 2016-07-20 angenommene Europäische Norm als DIN-Norm ist 2017-03-01.

Für DIN EN 61069-5:1995-09 besteht eine Übergangsfrist bis 2019-07-20.

Nationales Vorwort

Vorausgegangener Norm-Entwurf: E DIN EN 61069-5:2014-11.

Für dieses Dokument ist das nationale Arbeitsgremium K 931 „Systemaspekte“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik in DIN und VDE (www.dke.de) zuständig.

Die enthaltene IEC-Publikation wurde vom SC 65A „System aspects“ 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 ein Dokument ohne Angabe des Ausgabedatums und ohne Hinweis auf eine Abschnittsnummer, eine Tabelle, ein Bild usw.) bezieht sich die Verweisung auf die jeweils aktuellste Ausgabe des in Bezug genommenen Dokuments.

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

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

Änderungen

Gegenüber DIN EN 61069-5:1995-09 wurden folgende Änderungen vorgenommen:

- a) Überarbeitung der Begriffe. Sie wurden mit anderen Internationalen Normen abgeglichen, einige wurden neu hinzugefügt. Alle Begriffe sind jetzt in DIN EN 61069-1:2017 zusammengefasst.
- b) Inhalte von IEC/TS 62603-1:2014 übernommen. IEC/TC 65 beabsichtigt, mit Erscheinen der 2. Ausgabe der Normen der Reihe IEC 61069 den IEC/TS 62603-1:2014 zurückzuziehen. Er wurde nicht in das deutsche Normenwerk übernommen.
- c) Inhalte neu gegliedert. Innerhalb der Normenreihe IEC 61069 sind bestimmte Abschnitte und Unterabschnitte verschoben worden.
- d) Text überarbeitet.

Frühere Ausgaben

DIN EN 61069-5: 1995-09

Leittechnik für industrielle Prozesse –
Ermittlung der Systemeigenschaften zum Zweck der Eignungsbeurteilung
eines Systems –
Teil 5: Eignungsbeurteilung der Systemverlässlichkeit
(IEC 61069-5:2016)

Industrial-process measurement, control and
automation –
Evaluation of system properties for the purpose of
system assessment –
Part 5: Assessment of system dependability
(IEC 61069-5:2016)

Mesure, commande et automation dans les
processus industriels –
Appréciation des propriétés d'un système en vue
de son évaluation –
Partie 5: Evaluation de la sûreté de
fonctionnement d'un système
(IEC 61069-5:2016)

Diese Europäische Norm wurde von CENELEC am 2016-07-20 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

© 2016 CENELEC – Alle Rechte der Verwertung, gleich in welcher Form und in welchem Verfahren, sind weltweit den Mitgliedern von CENELEC vorbehalten.

Ref. Nr. EN 61069-5:2016 D

Europäisches Vorwort

Der Text des Dokuments 65A/793/FDIS, zukünftige 2. Ausgabe der IEC 61069-5, erarbeitet vom SC 65A „System aspects“ des IEC/TC 65 „Industrial-process measurement, control and automation“, wurde zur parallelen IEC-CENELEC-Abstimmung vorgelegt und von CENELEC als EN 61069-5:2016 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): 2017-04-20
- spätestes Datum, zu dem nationale Normen, die diesem Dokument entgegenstehen, zurückgezogen werden müssen (dow): 2019-07-20

Dieses Dokument ersetzt EN 61069-5:1995.

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 61069-5:2016 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 60300-3-1:2003	ANMERKUNG	Harmonisiert als EN 60300-3-1:2004 (nicht modifiziert).
IEC 60068 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN 60068.
IEC 60812:2006	ANMERKUNG	Harmonisiert als EN 60812:2006 (nicht modifiziert).
IEC 61000 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN 61000.
IEC 61025:2006	ANMERKUNG	Harmonisiert als EN 61025:2007 (nicht modifiziert).
IEC 61069-6	ANMERKUNG	Harmonisiert als EN 61069-6.
IEC 61078	ANMERKUNG	Harmonisiert als EN 61078.
IEC 61165	ANMERKUNG	Harmonisiert als EN 61165.
IEC 61326 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN 61326.
IEC 61508 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN 61508.
IEC 62443 (alle Teile)	ANMERKUNG	Harmonisiert in der Reihe EN 62443. ⁶⁾
IEC/TS 62603-1	ANMERKUNG	Harmonisiert als CLC/TS 62603-1.

⁶⁾ Im Entwurfsstadium.

Inhalt

	Seite
Europäisches Vorwort	2
Einleitung	6
1 Anwendungsbereich	8
2 Normative Verweisungen	8
3 Begriffe, Abkürzungen, Akronyme, Konventionen und Symbole	8
3.1 Begriffe	8
3.2 Abkürzungen, Akronyme, Konventionen und Symbole	8
4 Grundlagen der Eignungsbeurteilung in Bezug auf die Verlässlichkeit	9
4.1 Eigenschaften der Verlässlichkeit	9
4.1.1 Allgemeines	9
4.1.2 Verfügbarkeit	9
4.1.3 Zuverlässigkeit	10
4.1.4 Wartungsfreundlichkeit	10
4.1.5 Beherrschbarkeit	11
4.1.6 Sicherheit	11
4.1.7 Störunempfindlichkeit	11
4.2 Einflussfaktoren der Verlässlichkeit	12
5 Verfahren zur Eignungsbeurteilung	12
5.1 Allgemeines	12
5.2 Festlegung der Ziele der Eignungsbeurteilung	12
5.3 Entwurf und Ausgestaltung der Eignungsbeurteilung	13
5.4 Planung des Programms zur Eignungsbeurteilung	13
5.5 Durchführung der Eignungsbeurteilung	13
5.6 Bericht zur Eignungsbeurteilung	13
6 Ermittlungstechniken	14
6.1 Allgemeines	14
6.2 Analytische Ermittlungstechniken	15
6.2.1 Überblick	15
6.2.2 Induktives Analyseverfahren	15
6.2.3 Deduktives Analyseverfahren	15
6.2.4 Vorhersagende Ermittlung	15
6.3 Empirische Ermittlungstechniken	16
6.3.1 Überblick	16
6.3.2 Prüfungen mit Störungsinjektionstechniken	17
6.3.3 Prüfungen durch Störungen der Umgebung	17
6.4 Zusätzliche Themen für Ermittlungstechniken	17
Anhang A (informativ) Checkliste und/oder Beispiel des Lastenhefts für die Systemverlässlichkeit	18
Anhang B (informativ) Checkliste und/oder Beispiel des Pflichtenhefts für die Systemverlässlichkeit	19

	Seite
B.1 Informationen des Pflichtenhefts	19
B.2 Checkpunkte für die Systemverlässlichkeit	19
Anhang C (informativ) Beispiel für eine Liste von Elementen der Eignungsbeurteilung (Angaben aus IEC/TS 62603-1)	20
C.1 Überblick	20
C.2 Verlässlichkeit	20
C.3 Verfügbarkeit	20
C.3.1 Systemselbstdiagnose	20
C.3.2 Toleranz in Bezug auf Fehler einzelner Komponenten und Redundanz	20
C.3.3 Methoden der Redundanz	21
C.4 Zuverlässigkeit	23
C.5 Wartungsfreundlichkeit	23
C.5.1 Allgemeines	23
C.5.2 Generierung von Wartungsanforderungen	23
C.5.3 Wartungsstrategien	23
C.5.4 Wartung der Systemsoftware	23
C.6 Beherrschbarkeit	24
C.7 Sicherheit	24
C.8 Störunempfindlichkeit	24
C.8.1 Allgemeines	24
C.8.2 Hot-swap (Austausch im Betrieb)	24
C.8.3 Moduldiagnose	24
C.8.4 Eingabevalidierung	24
C.8.5 Abruffunktion	24
C.8.6 Erzwungene Ausgaben	25
C.8.7 Überwachungsfunktionen	25
C.8.8 Steuerung	25
C.8.9 Netzwerke	25
C.8.10 Arbeitsplatzrechner und Server	25
Anhang D (informativ) Beherrschbarkeitsprüfungen	26
D.1 Überblick	26
D.2 Injizierte Störungen	27
D.2.1 Allgemeines	27
D.2.2 Systemausfälle durch ein gestörtes Modul, Element oder eine gestörte Komponente	27
D.2.3 Systemausfälle durch menschliche Fehler	27
D.2.4 Systemausfälle durch falsche oder unberechtigte Eingaben in das System über die Mensch-Maschine-Schnittstelle	28
D.3 Beobachtungen	28
D.4 Auswertung der Ergebnisse	29

	Seite
Anhang E (informativ) Verfügbare Datenbanken zu Ausfallraten	30
E.1 Datenbanken	30
E.2 Nützliche Normen in Bezug auf den Ausfall von Komponenten	31
Anhang F (informativ) Sicherheitsbetrachtungen	32
F.1 Physische Sicherheit	32
F.2 Netzsicherheit	32
F.2.1 Allgemeines	32
F.2.2 Sicherheitspolitik	32
F.2.3 Weitere Betrachtungen	32
Literaturhinweise	34
Anhang ZA (normativ) Normative Verweisungen auf internationale Publikationen mit ihren entsprechenden europäischen Publikationen	36
 Bilder	
Bild 1 – Allgemeiner Aufbau der IEC 61069	7
Bild 2 – Verlässlichkeit	9

Einleitung

IEC 61069 behandelt die Methode, die zur Eignungsbeurteilung von Systemeigenschaften eines Basisleitsystems (BLS) verwendet werden sollte. IEC 61069 besteht aus den folgenden Teilen.

Teil 1: Terminologie und grundlegende Konzepte

Teil 2: Methodik der Eignungsbeurteilung

Teil 3: Eignungsbeurteilung der Systemfunktionalität

Teil 4: Eignungsbeurteilung des Systembetriebsverhaltens

Teil 5: Eignungsbeurteilung der Systemverlässlichkeit

Teil 6: Eignungsbeurteilung der Systembedienbarkeit

Teil 7: Eignungsbeurteilung der Systemsicherheit

Teil 8: Eignungsbeurteilung anderer Systemeigenschaften

Die Eignungsbeurteilung eines Systems ist eine Beurteilung, die auf dem Nachweis beruht, dass ein System für eine spezielle Aufgabe oder Klasse von Aufgaben geeignet ist.

Um einen vollständigen Nachweis zu erhalten (z. B. unter allen Einflussfaktoren), ist eine vollständige Ermittlung aller Systemeigenschaften erforderlich, die für die spezielle Aufgabe oder Klasse von Aufgaben relevant sind.

Da dies selten praktikabel ist, sollte die Eignungsbeurteilung eines Systems auf dem folgenden Grundprinzip beruhen:

- Bestimmung der kritischen Punkte einer jeden relevanten Systemeigenschaft;
- Planung der Ermittlung der relevanten Systemeigenschaften unter Berücksichtigung des Kostenaufwandes für die verschiedenen Systemeigenschaften.

Bei der Durchführung der Eignungsbeurteilung eines Systems muss die Notwendigkeit berücksichtigt werden, einen maximalen Vertrauenszuwachs in die Eignung eines Systems innerhalb praktikabler Zeit- und Kostenbegrenzungen zu erhalten.

Eine Eignungsbeurteilung kann nur durchgeführt werden, wenn eine Aufgabe festgelegt (oder angegeben) wurde oder wenn eine bestimmte Aufgabe angenommen werden kann. Ohne eine festgelegte Aufgabe kann keine Eignungsbeurteilung durchgeführt werden; für Eignungsbeurteilungen, die von Dritten vorgenommen werden, können jedoch Ermittlungen festgelegt und durchgeführt werden. In solchen Fällen kann IEC 61069 als Leitfaden für die Planung einer Ermittlung verwendet werden, da sie Methoden zur Durchführung von Ermittlungen vorgibt, welche wesentlicher Bestandteil einer Eignungsbeurteilung sind.

Bei der Vorbereitung der Eignungsbeurteilung kann festgestellt werden, dass die Definition des Systems zu eng gefasst ist. Bei einer Einrichtung mit zwei oder mehr Versionen des Leitsystems, welche gemeinsame Ressourcen wie ein Netzwerk nutzen, sollten beispielsweise Aspekte der Koexistenz und Interoperabilität berücksichtigt werden. In diesem Fall sollte das zu untersuchende System nicht auf das „neue“ BLS beschränkt sein, sondern beide Systeme einschließen. Das bedeutet, die Grenzen des Systems sollten derart verändert werden, dass das andere System ausreichend eingebunden wird, um diese Aspekte zu berücksichtigen.

Der Aufbau der Normenreihe und der Zusammenhang zwischen den Teilen von IEC 61069 sind in Bild 1 dargestellt.

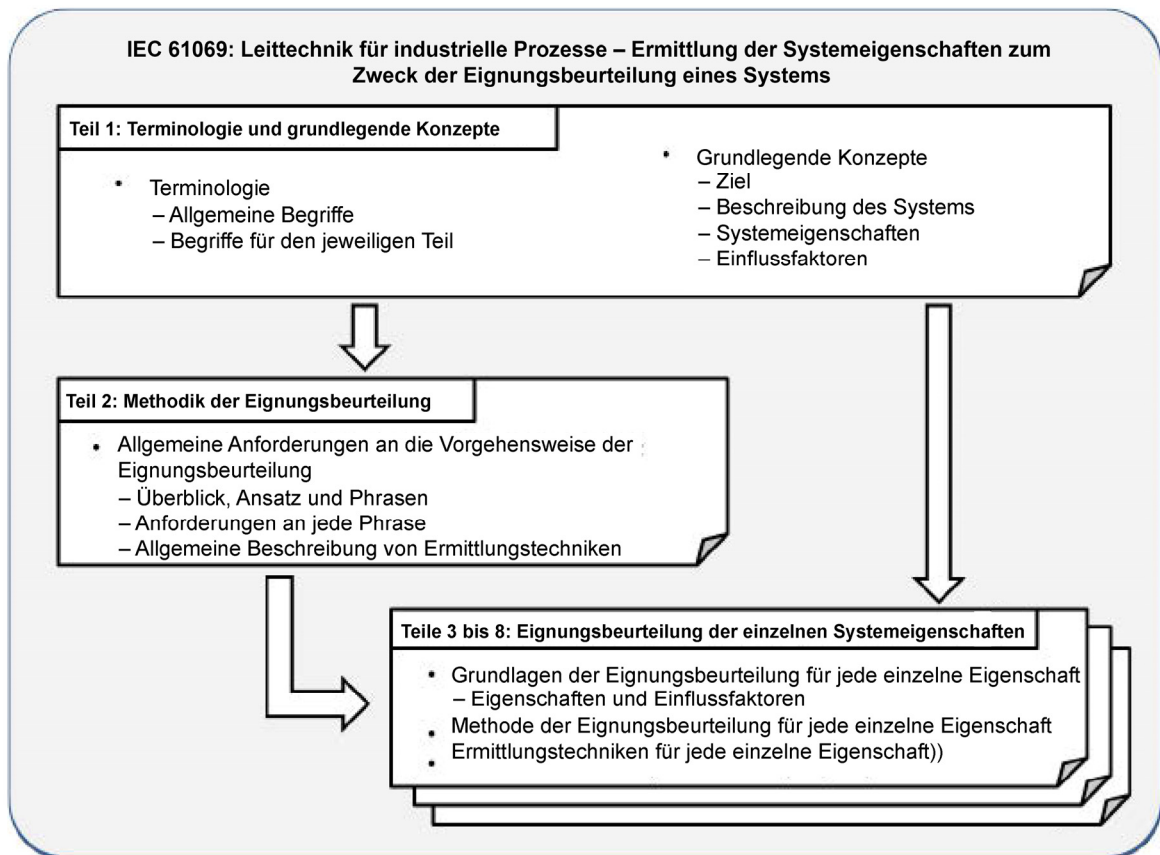


Bild 1 – Allgemeiner Aufbau der IEC 61069

Einige Beispiele für Elemente der Eignungsbeurteilung sind in Anhang C enthalten.

1 Anwendungsbereich

Dieser Teil von IEC 61069

- legt im Detail die Methode zur Eignungsbeurteilung der Verlässlichkeit eines Basisleitsystems (BLS) basierend auf den Konzepten nach IEC 61069-1 und der Methodik nach IEC 61069-2 fest,
- definiert eine grundlegende Kategorisierung der Eigenschaften der Verlässlichkeit,
- beschreibt die Faktoren, die die Verlässlichkeit beeinflussen und die bei der Ermittlung der Verlässlichkeit zu berücksichtigen sind, und
- bietet Leitlinien für die Auswahl von Techniken aus einer Reihe von Optionen (mit Verweisungen) für die Ermittlung der Verlässlichkeit.

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

IEC 60319, *Presentation and specification of reliability data for electronic components*

IEC 61069-1:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 1: Terminology and basic concepts*

IEC 61069-2:2016, *Industrial-process measurement, control and automation – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

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

IEC 61709:2011, *Electric components – Reliability – Reference conditions for failure rates and stress models for conversion*

ISO/IEC 25010, *Systems and software engineering – Systems and software Quality Requirements and Evaluation (SQuaRE) – System and software quality models*

ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements*

ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security controls*

3 Begriffe, Abkürzungen, Akronyme, Konventionen und Symbole

3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach IEC 61069-1.

3.2 Abkürzungen, Akronyme, Konventionen und Symbole

Für die Anwendung dieses Dokuments gelten die Abkürzungen, Konventionen und Symbole nach IEC 61069-1.

4 Grundlagen der Eignungsbeurteilung in Bezug auf die Verlässlichkeit

4.1 Eigenschaften der Verlässlichkeit

4.1.1 Allgemeines

Um die Verlässlichkeit vollständig beurteilen zu können, werden die Systemeigenschaften hierarchisch kategorisiert.

Um verlässlich zu sein, muss ein System zur Ausführung seiner Funktionen bereit sein. Allerdings bedeutet die Bereitschaft eines Systems, seine Funktion auszuführen, in der Praxis nicht, dass diese Funktionen mit Sicherheit richtig ausgeführt werden. Um diese beiden Aspekte zu berücksichtigen, werden die Eigenschaften der Verlässlichkeit in die Gruppen und Untergruppen aufgeteilt, die in Bild 2 dargestellt sind.

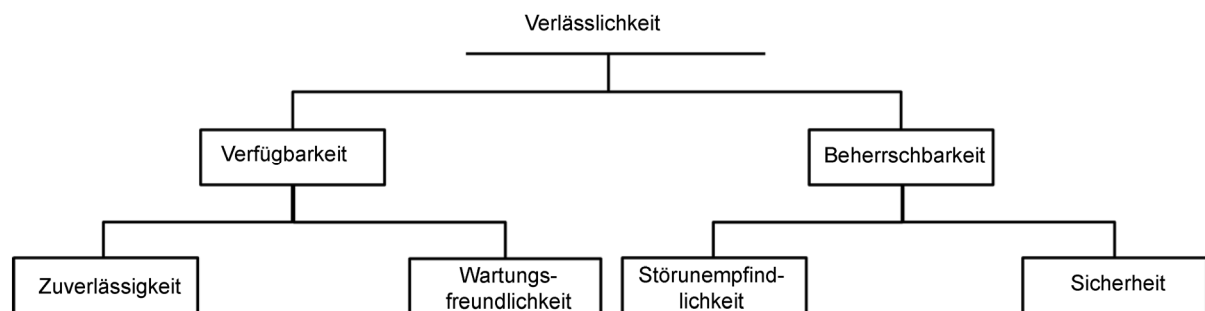


Bild 2 – Verlässlichkeit

Die Verlässlichkeit kann nicht direkt beurteilt und nicht durch eine einzelne Eigenschaft beschrieben werden. Die Verlässlichkeit kann nur durch individuelle Analyse und Prüfung jeder ihrer Eigenschaften bestimmt werden.

Der Zusammenhang zwischen den Verlässlichkeitseigenschaften des Systems und dessen Modulen ist mitunter sehr komplex.

Zum Beispiel:

- Wenn die Systemkonfiguration Redundanz einschließt, hängen die Verfügbarkeitseigenschaften des Systems von den Störune-mpfind-lichkeitseigenschaften der redundanten Module ab;
- wenn die Systemkonfiguration Sicherheitsmechanismen einschließt, hängen die Sicherheitseigenschaften des Systems von den Verfügbarkeitseigenschaften der Module ab, die die Sicherheitsmechanismen ausführen;
- wenn die Systemkonfiguration Module einschließt, die die Daten prüfen, die intern von anderen Systemteilen übertragen werden, hängt die Störune-mpfind-lichkeitseigenschaft des Systems von den Sicherheitseigenschaften dieser Module ab.

Wenn ein System mehrere Teilaufgaben des Systems ausführt, kann seine Verlässlichkeit für jede dieser Teilaufgaben anders sein. Für jede dieser Teilaufgaben ist eine getrennte Analyse erforderlich.

4.1.2 Verfügbarkeit

Die Verfügbarkeit des Systems ist von der Verfügbarkeit der einzelnen Module des Systems und der Art und Weise abhängig, in der diese Module bei der Ausführung der Teilaufgaben des Systems zusammenarbeiten. Die Art und Weise, wie diese Module des Systems zusammenarbeiten, kann die (homogene oder unterschiedliche) Funktionsredundanz, die Funktionssicherung und die Funktionsminderung einschließen. Die Verfügbarkeit des Systems ist in der Praxis von den eingesetzten Verfahren und den für den Weiterbetrieb des Systems verfügbaren Ressourcen abhängig. Die Verfügbarkeit des Systems kann im Hinblick auf seine einzelnen Teilaufgaben unterschiedlich sein.

Die Verfügbarkeit des Systems kann für jede Teilaufgabe auf zweierlei Weise quantifiziert werden:

Die Verfügbarkeit eines Systems kann wie folgt vorhergesagt werden:

$$\text{Verfügbarkeit} = \frac{\text{mittlere_Dauer_bis_zum_Ausfall}}{(\text{mittlere_Dauer_bis_zum_Ausfall} + \text{mittlere_Wiederherstellungsdauer})}$$

Dabei ist

- „Verfügbarkeit“ die Verfügbarkeit des Systems für eine gegebene Teilaufgabe;
- „die_mittlere_Dauer_bis_zum_Ausfall“ der Mittelwert der Zeit von der Wiederherstellung des Systems in einen Zustand, in dem es die gegebene(n) Teilaufgabe(n) ausführt, bis zu dem Zeitpunkt, an dem das System ausfällt;
- die „mittlere_Wiederherstellungsdauer“ der Mittelwert der Gesamtzeit, die zur Wiederherstellung der Ausführung der gegebenen Teilaufgabe erforderlich ist, und zwar von dem Zeitpunkt an, an dem das System beim Ausführen jener Teilaufgabe ausfiel.

Für ein System im Betrieb kann die Verfügbarkeit wie folgt berechnet werden:

$$\text{Verfügbarkeit} = \frac{\text{Gesamtzeit_während_der_das_System_die_gegebene_Teilaufgabe_ausführen_konnte}}{\text{Gesamtzeit_während_der_vom_System_die_Ausführung_der_Teilaufgabe_erwartet_wurde}}$$

4.1.3 Zuverlässigkeit

Die Zuverlässigkeit eines Systems ist von der Zuverlässigkeit der einzelnen Module des Systems und der Art und Weise abhängig, in der diese Module bei der Ausführung der Teilaufgaben des Systems zusammenarbeiten. Die Art und Weise, wie diese Module zusammenarbeiten, kann die (homogene oder unterschiedliche) Funktionsredundanz, die Funktionssicherung und die Funktionsminderung einschließen.

Die Zuverlässigkeit des Systems kann im Hinblick auf seine einzelnen Teilaufgaben unterschiedlich sein. Die Zuverlässigkeit kann für einzelne Teilaufgaben quantitativ bestimmt werden, wobei der Grad des Vertrauens in diese Vorhersage variiert.

Die Zuverlässigkeit der einzelnen Elemente des Systems kann mithilfe des Teilezählverfahrens vorhergesagt werden (siehe IEC 62380 und IEC 61069-6). Die Zuverlässigkeit des Systems kann daraufhin durch Synthese vorhergesagt werden. Es sollte beachtet werden, dass die für die Softwaremodule von Systemen zur Verfügung stehenden Verfahren zur Vorhersage der Zuverlässigkeit keine hohen Vertrauensgrade erreichen.

Verfahren zur Analyse der Softwarezuverlässigkeit werden in ISO/IEC 25010 beschrieben.

Die Zuverlässigkeit kann anhand der mittleren Dauer bis zum Ausfall (MTTF) oder der Ausfallrate dargestellt werden.

4.1.4 Wartungsfreundlichkeit

Die Wartungsfreundlichkeit eines Systems ist von der Wartungsfreundlichkeit der einzelnen Elemente sowie der Struktur der Elemente und Module des Systems abhängig. Die physikalische Struktur beeinflusst die Leichtigkeit des Zugangs, der Austauschbarkeit usw. Die funktionelle Struktur beeinflusst die Leichtigkeit der Diagnose usw.

Bei der quantitativen Bestimmung der Wartungsfreundlichkeit eines Systems sollten alle Tätigkeiten berücksichtigt werden, die erforderlich sind, um das System in den Zustand zurückzusetzen, in dem es seine Teilaufgaben vollständig ausführen kann. Dazu sollten Tätigkeiten gehören, wie die erforderliche Zeit zur Erkennung des Fehlers, zur Anzeige der Wartung, zur Diagnose und Behebung der Ursache, zum Abgleich und zur Überprüfung usw.

Die quantitative Bestimmung der Wartungsfreundlichkeit sollte durch qualitative Aussagen ergänzt werden, indem die Bereitstellung und Abdeckung der folgenden Punkte überprüft wird: