

**DIN EN 61069-5**

ICS 35.240.50

Einsprüche bis 2014-12-03  
Vorgesehen als Ersatz für  
DIN EN 61069-5:1995-09

**Entwurf**

**Leittechnik für industrielle Prozesse –  
Ermittlung der Systemeigenschaften zum Zweck der  
Eignungsbeurteilung eines Systems –  
Teil 5: Eignungsbeurteilung der Systemverlässlichkeit  
(IEC 65A/676/CD:2014)**

Industrial-process measurement and control –  
Evaluation of system properties for the purpose of system assessment –  
Part 5: Assessment of system dependability  
(IEC 65A/676/CD:2014)

**Anwendungswarnvermerk**

Dieser Norm-Entwurf mit Erscheinungsdatum 2014-10-03 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](http://www.entwuerfe.din.de) bzw. für Norm-Entwürfe der DKE auch im Norm-Entwurfs-Portal der DKE unter [www.entwuerfe.normenbibliothek.de](http://www.entwuerfe.normenbibliothek.de), sofern dort wiedergegeben;
- oder als Datei per E-Mail an [dke@vde.com](mailto:dke@vde.com) möglichst in Form einer Tabelle. Die Vorlage dieser Tabelle kann im Internet unter [www.din.de/stellungnahme](http://www.din.de/stellungnahme) oder für Stellungnahmen zu Norm-Entwürfen der DKE unter [www.dke.de/stellungnahme](http://www.dke.de/stellungnahme) abgerufen werden;
- oder in Papierform an die DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im 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 38 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

## Inhalt

|                                                                                                                                                  | Seite |
|--------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| Nationales Vorwort.....                                                                                                                          | 5     |
| Einleitung .....                                                                                                                                 | 6     |
| 1 Anwendungsbereich.....                                                                                                                         | 8     |
| 2 Normative Verweisungen .....                                                                                                                   | 8     |
| 3 Begriffe, Abkürzungen, Konventionen und Symbole.....                                                                                           | 9     |
| 3.1 Begriffe .....                                                                                                                               | 9     |
| 3.2 Abkürzungen, Konventionen und Symbole .....                                                                                                  | 9     |
| 4 Grundlagen der Eignungsbeurteilung in Bezug auf die Verlässlichkeit .....                                                                      | 9     |
| 4.1 Eigenschaften der Verlässlichkeit .....                                                                                                      | 9     |
| 4.2 Einflussfaktoren der Verlässlichkeit.....                                                                                                    | 12    |
| 5 Verfahren zur Eignungsbeurteilung.....                                                                                                         | 13    |
| 5.1 Allgemeines .....                                                                                                                            | 13    |
| 5.2 Festlegung der Ziele der Eignungsbeurteilung .....                                                                                           | 13    |
| 5.3 Entwurf und Ausgestaltung der Eignungsbeurteilung .....                                                                                      | 13    |
| 5.4 Entwurf des Programms zur Eignungsbeurteilung.....                                                                                           | 14    |
| 5.5 Durchführung der Eignungsbeurteilung.....                                                                                                    | 15    |
| 5.6 Bericht zur Eignungsbeurteilung .....                                                                                                        | 15    |
| 6 Ermittlungstechniken .....                                                                                                                     | 15    |
| 6.1 Allgemeines .....                                                                                                                            | 15    |
| 6.2 Analytische Ermittlungstechniken.....                                                                                                        | 16    |
| 6.3 Empirische Ermittlungstechniken .....                                                                                                        | 18    |
| 6.4 Zusätzliche Themen für Ermittlungstechniken .....                                                                                            | 19    |
| Anhang A (informativ) Lastenheft (Checkliste, Beispiel usw.).....                                                                                | 20    |
| Anhang B (informativ) Pflichtenheft (Checkliste, Beispiel usw.).....                                                                             | 21    |
| Anhang C (informativ) Dokument mit zusammengestellten Informationen (Checkliste, Beispiel usw.).....                                             | 22    |
| Anhang D (informativ) Matrix zur Eignungsbeurteilung .....                                                                                       | 23    |
| Anhang E (informativ) Teil 5 – 4 Eigenschaften der Verlässlichkeit; Beispielhafte Informationen einer Systemspezifikation aus IEC/TS 62603 ..... | 24    |
| E.1 Teil 5 – 4.1 Allgemeines .....                                                                                                               | 24    |
| E.2 Teil 5 – 4.2 Verlässlichkeit.....                                                                                                            | 24    |
| E.3 Teil 5 – 4.3 Verfügbarkeit .....                                                                                                             | 24    |
| E.3.1 Systemselbstdiagnose.....                                                                                                                  | 24    |
| E.3.2 Toleranz in Bezug auf Fehler einzelner Komponenten und Redundanz .....                                                                     | 25    |
| E.3.3 Schutzmaßnahme im ausfallsicheren Betrieb .....                                                                                            | 26    |
| E.3.4 Im Betrieb austauschbare Komponenten.....                                                                                                  | 26    |
| E.4 Teil 5 – 4.4 Zuverlässigkeit.....                                                                                                            | 27    |

|                                                                                                                                                                       | Seite |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------|
| E.5 Teil 5 – 4.5 Wartungsfreundlichkeit.....                                                                                                                          | 27    |
| E.5.1 Generierung von Wartungsanforderungen .....                                                                                                                     | 27    |
| E.5.2 Wartungsstrategien .....                                                                                                                                        | 27    |
| E.5.3 Wartung der Systemsoftware.....                                                                                                                                 | 27    |
| E.6 Teil 5 – 4.6 Beherrschbarkeit .....                                                                                                                               | 28    |
| E.7 Teil 5 – 4.7 Sicherheit .....                                                                                                                                     | 28    |
| E.8 Teil 5 – 4.8 Störunempfindlichkeit.....                                                                                                                           | 28    |
| E.8.1 Hot-Swap (Austausch im Betrieb).....                                                                                                                            | 28    |
| E.8.2 Moduldiagnose .....                                                                                                                                             | 28    |
| E.8.3 Eingabvalidierung.....                                                                                                                                          | 28    |
| E.8.4 Abruffunktion .....                                                                                                                                             | 28    |
| E.8.5 Erzwungene Ausgaben .....                                                                                                                                       | 29    |
| E.8.6 Überwachungsfunktionen.....                                                                                                                                     | 29    |
| E.8.7 E/A-Netzwerk .....                                                                                                                                              | 29    |
| E.8.8 Regler.....                                                                                                                                                     | 29    |
| E.8.9 Prozessleitnetzwerk .....                                                                                                                                       | 29    |
| E.8.10 Arbeitsplatzrechner und Server.....                                                                                                                            | 29    |
| Anhang F (informativ) Beispiel der benötigten Informationen und des Dokumentationsformats für<br>eine Master-Slave-Steuerungs-Teilaufgabe in einem Lastenheft.....    | 30    |
| F.1 Schematische Darstellung der Teilaufgabe .....                                                                                                                    | 30    |
| F.2 Grenzzustände.....                                                                                                                                                | 30    |
| Anhang G (informativ) Beispiel der benötigten Informationen und des Dokumentationsformats für<br>eine Master-Slave-Steuerungs-Teilaufgabe in einem Pflichtenheft..... | 32    |
| G.1 32                                                                                                                                                                |       |
| Anhang H (informativ) Beherrschbarkeitsprüfungen .....                                                                                                                | 34    |
| H.1 Einleitung.....                                                                                                                                                   | 34    |
| H.2 Injizierte Störungen .....                                                                                                                                        | 35    |
| H.2.1 Systemausfälle durch ein gestörtes Modul, Element oder eine gestörte Komponente .....                                                                           | 35    |
| H.2.2 Systemausfälle durch menschliche Fehler .....                                                                                                                   | 35    |
| H.2.3 Systemausfälle durch falsche oder unberechtigte Eingaben in das System über die Mensch-<br>Maschine-Schnittstelle .....                                         | 35    |
| H.3 Beobachtungen .....                                                                                                                                               | 36    |
| H.4 Auswertung der Ergebnisse .....                                                                                                                                   | 36    |
| Anhang I (informativ) (Optional): Andere eigenschaftsspezifische Themen .....                                                                                         | 37    |
| Literaturhinweise .....                                                                                                                                               | 38    |
| <b>Bilder</b>                                                                                                                                                         |       |
| Bild 1 – Allgemeiner Aufbau der IEC 61069.....                                                                                                                        | 7     |
| Bild 2 – Hierarchie der Eigenschaften der Verlässlichkeit.....                                                                                                        | 9     |
| Bild F.1 – Verlässlichkeit .....                                                                                                                                      | 24    |
| Bild A.1 – Schematische Darstellung der Teilaufgabe .....                                                                                                             | 30    |

|                                     | Seite |
|-------------------------------------|-------|
| <b><u>Tabellen</u></b>              |       |
| Tabelle E.1 – Verlässlichkeit.....  | 31    |
| Tabelle G.1 – Verlässlichkeit ..... | 32    |

## Nationales Vorwort

Das internationale Dokument IEC 65A/676/CD:2014 „Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 5: Assessment of system dependability“ (CD, en: Committee Draft) ist unverändert in diesen Norm-Entwurf übernommen worden. Dieser Norm-Entwurf enthält eine autorisierte deutsche Übersetzung.

Das internationale Dokument wurde vom SC 65A „System aspects“ 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 931 „Systemaspekte“ der DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE ([www.dke.de](http://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 Abschnichtsnummer, 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.

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.

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.

## Änderungen

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

- Überarbeitung der Begriffe. Sie wurden mit anderen internationalen Normen abgeglichen, einige wurden neu hinzugefügt. Alle Begriffe sind jetzt in Teil 1 der Reihe DIN EN 61069 zusammengefasst;
- 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;
- Inhalte neu gegliedert. Innerhalb der Normenreihe IEC 61069 sind bestimmte Abschnitte verschoben worden;
- Textlich überarbeitet.

**Leittechnik für industrielle Prozesse –  
Ermittlung der Systemeigenschaften zum Zweck der Eignungsbeurteilung eines  
Systems –  
Teil 5: Eignungsbeurteilung der Systemverlässlichkeit**

## Einleitung

Dieser Teil von IEC 61069 behandelt die Methode, die zur Eignungsbeurteilung anderer Systemeigenschaften von Basisleitsystemen (BLS) verwendet werden sollte.

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 Eigenschaften.

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 (nach der Definition in IEC 61069-1) festgelegt und durchgeführt werden.

In solchen Fällen kann die Norm 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 wird möglicherweise festgestellt, 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 Zusammenhang zwischen diesem Teil und den anderen Teilen von IEC 61069 sowie die entsprechende Position dieses Teils innerhalb der Norm ist in Bild 1 veranschaulicht.

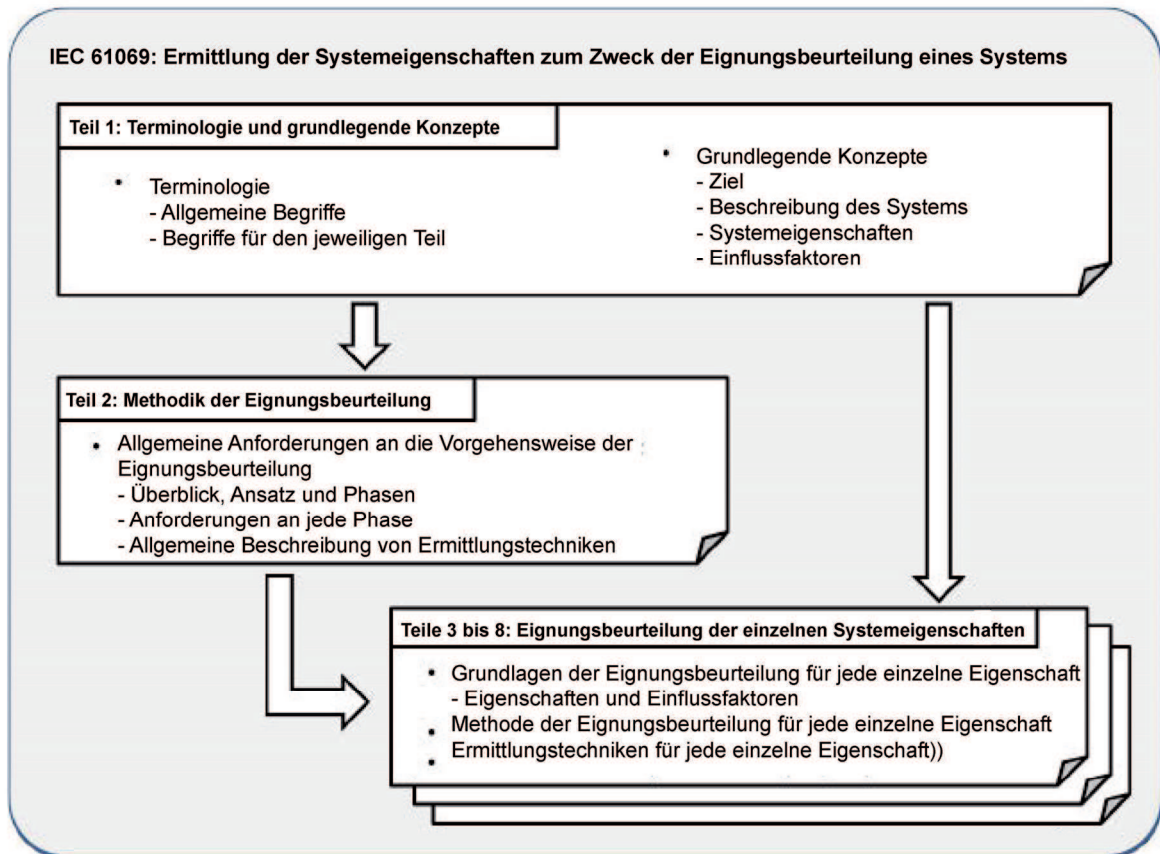


Bild 1 – Allgemeiner Aufbau der IEC 61069

## 1 Anwendungsbereich

Dieser Teil von IEC 61069 legt im Detail die Methode zur Eignungsbeurteilung der Systemverlässlichkeit eines Basisleitsystems (BLS) fest.

Die untergeordneten Eigenschaften der Systemverlässlichkeit werden analysiert und es werden Kriterien beschrieben, die bei der Eignungsbeurteilung der Verlässlichkeit zu berücksichtigen sind.

Es wird auf andere ergänzende Ermittlungstechniken verwiesen.

## 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).

Anmerkung des Bearbeiters: Richtiges Datum hinzufügen, sobald verfügbar.

IEC 60050, *International Electrotechnical Vocabulary (IEV) – Chapter 191: Dependability and quality of service*

IEC 60068, *Environmental testing*

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

IEC 60706-4, *Guide on maintainability of equipment – Part 4: Section 8: Maintenance and maintenance support planning*

IEC 60801, *Electromagnetic compatibility for industrial-process measurement and control equipment*

IEC 60812:1985, *Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA)*

IEC 60863, *Presentation of reliability, maintainability and availability predictions*

IEC 61000, *Electromagnetic compatibility (EMC)*

IEC 61025:1990, *Fault tree analysis (FTA)*

IEC 61069-1:1991, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 1: General considerations and methodology*

IEC 61069-2:1993, *Industrial-process measurement and control – Evaluation of system properties for the purpose of system assessment – Part 2: Assessment methodology*

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

IEC 61078, *Analysis techniques for dependability – Reliability block diagram method IEC 1132:199x, Failure rate prediction of items having a series structure (in Bearbeitung) IEC 1165:199x, Application of Markov techniques (in Bearbeitung)*

ISO/IEC 27001 und ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security management (ISMS)*

### 3 Begriffe, Abkürzungen, Konventionen und Symbole

#### 3.1 Begriffe

Für die Anwendung dieses Dokuments gelten die Begriffe nach Teil 1 und die folgenden Begriffe.

Für die Anwendung dieser Ausgabe werden keine zusätzlichen Begriffe benötigt.

#### 3.2 Abkürzungen, Konventionen und Symbole

Für die Anwendung dieser Ausgabe werden keine zusätzlichen Abkürzungen, Konventionen und Symbole benötigt.

### 4 Grundlagen der Eignungsbeurteilung in Bezug auf die Verlässlichkeit

#### 4.1 Eigenschaften der Verlässlichkeit

##### 4.1.1 Allgemeines

Um verlässlich zu sein, muss ein System zur Ausführung seiner Funktionen bereit sein. Dies ist eine Frage der Verfügbarkeit und hängt von der Häufigkeit der Systemausfälle (Zuverlässigkeit) und der Zeit, die zur Wiederherstellung des Systems erforderlich ist (Wartungsfreundlichkeit), ab.

Allerdings bedeutet die Bereitschaft eines Systems, seine Funktion auszuführen, in der Praxis nicht, dass diese Funktionen mit Sicherheit richtig ausgeführt werden.

Dies ist eine Frage der Beherrschbarkeit, die abhängt von:

- der Fähigkeit des Systems, Warnungen zu geben, falls es in einen Zustand fallen sollte, in dem es nicht in der Lage ist, einige oder alle seine Funktionen ordnungsgemäß auszuführen (Störunempfindlichkeit);
- der Fähigkeit des Systems, falsche Eingangssignale oder unberechtigte Zugriffe zurückzuweisen (Sicherheit).

Um die Verlässlichkeit eines Systems zu beurteilen, ist es daher erforderlich, die untergeordneten Eigenschaften, die die Verlässlichkeit bestimmen, zu ermitteln und zu beurteilen.

Der Zusammenhang zwischen der Verlässlichkeit und ihren untergeordneten Eigenschaften ist in Bild 2 dargestellt.

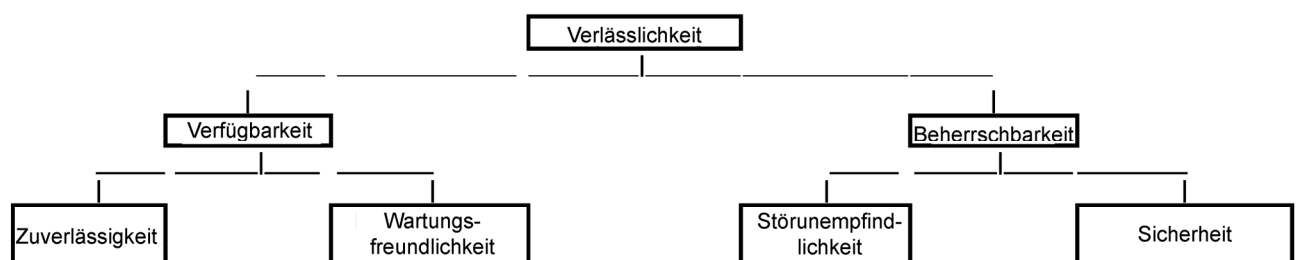


**Bild 2 – Hierarchie der Eigenschaften der Verlässlichkeit**

##### 4.1.2 Verlässlichkeit

Die Verlässlichkeit kann nicht direkt beurteilt werden. Es ist notwendig, jede der untergeordneten Eigenschaften einzeln zu beurteilen.

Jede untergeordnete Eigenschaft hängt von der Anordnung der Systemmodule in der Gesamtarchitektur und den Verlässlichkeitseigenschaften dieser Module ab.

Der Zusammenhang zwischen den untergeordneten Verlässlichkeitseigenschaften dieser Module und der Verlässlichkeit des Systems kann sehr komplex sein.

Jede untergeordnete Eigenschaft auf Systemebene kann von mehreren untergeordneten Eigenschaften auf Modulebene abhängen.

Zum Beispiel:

- wenn die Systemkonfiguration Redundanz einschließt, hängt die Systemverfügbarkeit von den Störungs-empfindlichkeitseigenschaften der redundanten Module ab;
- wenn die Systemkonfiguration Sicherheitsmechanismen einschließt, hängt die Systemsicherheit 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 Störungs-empfindlichkeit des Systems von den Sicherheitseigenschaften dieser Module ab.

Verlässlichkeit kann nicht durch eine einzelne Zahl beschrieben werden. Einige ihrer Eigenschaften können als Wahrscheinlichkeiten ausgedrückt werden, andere Eigenschaften sind deterministisch, einige Aspekte können quantifiziert werden, andere Aspekte können nur in einer qualitativen Weise beschrieben werden.

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

#### 4.1.3 Verfügbarkeit

Die Verfügbarkeit des Systems ist von der Verfügbarkeit der einzelnen Teile des Systems und der Art und Weise abhängig, in der diese Teile bei der Ausführung der Teilaufgaben des Systems zusammenarbeiten. Die Art und Weise, wie diese Teile 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.

##### 4.1.3.1 Vorhersage der Verfügbarkeit

Die Verfügbarkeit eines Systems kann wie folgt berechnet 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.

##### 4.1.3.2 Berechnung der Verfügbarkeit

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

$$\text{Verfügbarkeit} = \frac{\text{Gesamtzeit, während der das System die gegebene Teilaufgabe ausführen konnte}}{\text{Gesamtzeit, während der vom System die Ausführung der Teilaufgabe erwartet wurde}}$$

#### 4.1.4 Zuverlässigkeit

Die Zuverlässigkeit eines Systems ist von der Zuverlässigkeit der einzelnen Teile des Systems und der Art und Weise abhängig, in der diese Teile bei der Ausführung der Teilaufgaben des Systems zusammenarbeiten. Die Art und Weise, wie diese Teile 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 Hardwareteile des Systems kann mithilfe des Teilezählverfahrens vorhergesagt werden. 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 4.6 des Internationalen Sekretariatsentwurfs IEC 56(Sekretariat)319 „Software reliability and maintainability requirements analysis“ (in Bearbeitung) beschrieben. (Anmerkung des Bearbeiters: Verweisung auflösen)

#### 4.1.5 Wartungsfreundlichkeit

Die Wartungsfreundlichkeit eines Systems ist von der Wartungsfreundlichkeit der einzelnen Teile sowie der physikalischen und funktionellen Struktur 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 gehören Tätigkeiten 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:

- Anzeige des Auftretens eines Ausfalls: Lichtsignale, Alarmmeldungen, Berichte usw.;
- Zugang: Leichtigkeit des Zugangs für das Personal und für den Anschluss von Messinstrumenten, Modularität usw.;
- Diagnose: direkte Fehlererkennung, rückwirkungsfreie Diagnosewerkzeuge, fernbediente Möglichkeiten der Wartungsunterstützung, statistische Fehlerprüfung und -aufzeichnung;
- Reparierbarkeit/Austauschbarkeit: geringe Einschränkungen des Austausches von Modulen im Betrieb („Hot-Swap“-Unterstützung) Modularität, eindeutige Kennzeichnung der Module und Elemente, minimales Erfordernis von Spezialwerkzeugen, minimale Rückwirkungen auf andere Elemente oder Module, wenn Elemente oder Module ersetzt werden;
- Prüfung: angeleitete Wartungsverfahren, minimale Prüfungsanforderungen.

#### 4.1.6 Beherrschbarkeit

Die Beherrschbarkeit eines Systems ist von den Störungsempfindlichkeits- und Sicherheitsmechanismen abhängig, die als Funktionen, die von den Systemteilen ausgeführt werden, implementiert sind.

Ein Störungsempfindlichkeitsmechanismus wird durch ein Element implementiert, das die Ausgänge anderer Elemente überprüft.

Ein Sicherheitsmechanismus wird durch ein Element implementiert, das die Eingänge anderer Elemente überprüft.

Beherrschbarkeitsmechanismen schließen Folgendes ein:

- eine Überprüfung auf
  - die richtige Ausführung von Funktionen (z. B. durch eine Zeitüberwachungseinrichtung, die Verwendung bekannter Daten); und/oder
  - richtige Daten (z. B. Gültigkeitsprüfung, Paritätsprüfung, Rücklesbarkeit, Eingabeprüfung usw.);
- eine Tätigkeit, wie:
  - Selbstkorrektur;
  - Begrenzung;
  - Anzeige der Tätigkeit usw.

Diese Mechanismen können verwendet werden, um Störunempfindlichkeit und/oder Sicherheit zu erreichen.

Um Beherrschbarkeitsmechanismen zu analysieren, können die in 6.1 beschriebenen Fehlerinjektionsverfahren angewendet werden.

Die Beherrschbarkeit ist deterministisch und einige Aspekte können quantitativ bestimmt werden.

#### 4.1.7 Sicherheit

Die Sicherheit eines Systems ist von Mechanismen abhängig, die an den Systemgrenzen zur Erkennung und Verhinderung fehlerhafter Eingangssignale und unberechtigter Zugriffe implementiert sind. Diese Systemgrenzen können physikalisch sein oder online bestehen. Siehe Anhang E für einen kurzen Überblick über zu berücksichtigende Punkte.

Einige Aspekte der Sicherheit sind deterministisch. Diese Aspekte können quantitativ bestimmt werden.

#### 4.1.8 Störunempfindlichkeit

Die Störunempfindlichkeit ist von Mechanismen abhängig, die an den Ausgabeelementen des Systems implementiert sind, um die Richtigkeit der Ausgangssignale zu prüfen. Sie ist außerdem von Mechanismen abhängig, die innerhalb des Systems zur Erkennung und Zurückweisung von fehlerhaften Übergängen von Signalen oder Daten zwischen Teilen des Systems implementiert sind. Diese internen Mechanismen sind Störunempfindlichkeits- oder Sicherheitsmechanismen in Bezug auf die zugeordneten Teile, von denen jedes als ein eigenes System betrachtet werden kann.

Die Störunempfindlichkeit ist deterministisch und einige Aspekte können quantitativ bestimmt werden.

### 4.2 Einflussfaktoren der Verlässlichkeit

Die Verlässlichkeit eines Systems kann durch die folgenden Einflussfaktoren, die in 5.3 von IEC 61069-1 aufgeführt sind, beeinflusst werden.

Für jede der in 4.1 aufgeführten untergeordneten Eigenschaften gelten die folgenden primären Einflussfaktoren.

- Die Zuverlässigkeit wird durch die folgenden Einflussfaktoren beeinflusst:
  - Versorgungseinrichtungen, deren Einfluss mithilfe des Internationalen Sekretariatsentwurfs IEC 56(Sekretariat)383 „Use of failure rate data intended for reliability prediction of components in electronic equipment – Reference conditions – Stress models for their conversion“ (in Bearbeitung) teilweise vorhersagbar ist; (Anmerkung des Bearbeiters: Verweisung auflösen)
  - Umgebung, deren Einfluss mithilfe des Internationalen Sekretariatsentwurfs IEC 56(Sekretariat)383 teilweise vorhersagbar ist; (Anmerkung des Bearbeiters: Verweisung auflösen)
  - Dienstleistungen, durch Handhabung, Lagerung von Teilen usw.;