Definitionen von Begriffen im Kontext ‚Sicherheit (safety)'

Udo Voges
Forschungszentrum Karlsruhe
Institut für Angewandte Informatik
Postfach 3640
76021 Karlsruhe
Tel. +49-(0)7247-82-5725
email: voges@iai.fzk.de

Im Folgenden wird ein Überblick über verschiedene Begriffe und deren Definitionen im Kontext von Sicherheit im Sinne von Safety gegeben. Dabei wird ersichtlich, dass kein einheitliches Begriffs- und Definitionen-Gerüst besteht, sondern in verschiedenen Bereichen z.T. von unterschiedlichen Definitionen und Begriffsbestimmungen ausgegangen wird. Dies trifft nicht nur bei der Abbildung des deutschen Sprachgebrauchs auf die englische Verwendung zu.

A. Definitionen gemäß DIN EN 61508-4: August 2002 /DIN2002/

3.1 Sicherheitsbezogene Begriffe

3.1.1 Schaden (en: harm)
physische Verletzung oder Schädigung der Gesundheit von Menschen, entweder direkt oder indirekt als ein Ergebnis von Schäden von Gütern oder der Umwelt
[ISO/IEC Guide 51:1990 (modifiziert)]

3.1.2 Gefährdung (en: hazard)
potentielle Schadensquelle [ISO/IEC Guide 51:1990]
ANMERKUNG Der Begriff schließt die Gefährdungen von Personen ein, die innerhalb einer kurzen Zeitspanne entstehen (zum Beispiel durch Feuer und Explosion) und auch die, die eine Langzeitwirkung auf die Gesundheit einer Person haben (zum Beispiel durch Freisetzung einer giftigen Substanz).

3.1.3 Gefährdungssituation (en: hazardous situation)
Umstand, durch den eine Person einer Gefährdung ausgesetzt ist

3.1.4 Gefährlicher Vorfall (en: hazardous event)
Gefährdungssituation, die zu einem Schaden führt

3.1.5 Risiko (en: risk)
Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens [ISO/IEC Guide 51:1990 (modifiziert)]
ANMERKUNG Für die weitere Diskussion dieses Begriffs siehe Anhang A von IEC 61508-5.

3.1.6 Tolerierbares Risiko (en: tolerable risk)
Risiko, das basierend auf den aktuellen gesellschaftlichen Wertvorstellungen in einem gegebenen Zusammenhang tragbar ist
ANMERKUNG Siehe Anhang B von IEC 61508-5.

3.1.7 Restrisiko (en: residual risk)
Das trotz Schutzmaßnahmen verbleibende Risiko

3.1.8 Sicherheit (en: safety)
Freiheit von unvertretbaren Risiken
(Anmerkung uv: entspricht auch ISO/IEC Guide 51:1999, Definition 3.1)

3.1.9 Funktionale Sicherheit (en: functional safety)
Teil der Gesamtsicherheit, bezogen auf die EUC und das EUC-Leit- oder Steuerungssystem, die von der korrekten Funktion des E/E/PE-sicherheitsbezogenen Systems, sicherheitsbezogenen Systemen anderer Technologie und externer Einrichtungen zur Risikominderung abhängt

3.1.10 Sicherer Zustand (en: safe state)
Zustand der EUC, in dem die Sicherheit erreicht ist
ANMERKUNG Beim Übergang von einem potentiell gefährlichen Zustand zum endgültigen sicheren Zustand kann die EUC eine Anzahl von Sicherheits-Zwischenzuständen durchlaufen. Für einige Situationen existiert ein sicherer

Zustand nur so lange, wie die EUC einer ununterbrochenen Steuerung unterliegt. Solche eine ununterbrochene Steuerung kann für eine kurze oder einen unbestimmten Zeitraum erfolgen.

3.1.11 Vernünftigerweise vorhersehbare Fehlanwendung (en: reasonably foreseeable misuse)
Verwendung eines Produktes, Verfahrens oder einer Dienstleistung unter Bedingungen oder für Zwecke, die von einem Lieferer nicht vorgesehen sind, sondern die, verursacht durch das Produkt, das Verfahren oder die Dienstleistung, in Verbindung mit oder als ein Ergebnis von üblichen menschlichen Verhaltensweisen geschehen können

B. Definitionen gemäß DIN EN 14971: 2001 /DIN2001/

2 Begriffe und Definitionen

2.2 Schaden
physische Verletzung oder Schädigung der Gesundheit von Menschen oder Schädigung von Gütern oder der Umwelt
[ISO/IEC Guide 51:1999, Definition 3.3]

2.3 Gefährdung
potentielle Schadensquelle
[ISO/IEC Guide 51:1999, Definition 3.5]

2.4 Gefährdungssituation
Zustand, in dem Menschen, Güter oder die Umwelt einer oder mehreren Gefährdungen ausgesetzt sind
[ISO/IEC Guide 51:1999, Definition 3.6]

2.5 Bestimmungsgemäßer Gebrauch/Zweckbestimmung
Anwendung eines Produkts, eines Verfahrens oder einer Leistung nach den durch den HERSTELLER gelieferten Spezifikationen, Anweisungen und Angaben

2.8 Nachweis
Information, deren Richtigkeit bewiesen werden kann, und die auf der Tatsache beruht, welche durch Beobachtung, Messung, Untersuchung oder durch andere Ermittlungsverfahren gewonnen sind
[ISO 8402:1994, Definition 2.19]

2.9 Verfahren
festgelegte Art und Weise, eine Tätigkeit auszuführen
[ISO 8402:1994, Definition 1.3]

2.10 Prozess
Satz von in Wechselbeziehungen stehenden Mitteln und Tätigkeiten, die Eingaben in Ergebnisse umgestalten
[ISO 8402:1994, Definition 1.2]

2.12 Restrisiko
Risiko, das nach der Anwendung von Schutzmaßnahmen verbleibt
[ISO/IEC Guide 51:1999, Definition 3.9]

2.13 Risiko
Kombination der Wahrscheinlichkeit des Auftretens eines SCHADENS und des SCHWEREGRADES dieses SCHADENS
[ISO/IEC Guide 51:1999, Definition 3.2]

2.14 Risikoanalyse
systematische Auswertung verfügbarer Informationen, um Gefährdungen zu identifizieren und RISIKEN abzuschätzen
[ISO/IEC Guide 51:1999, Definition 3.10]

2.15 Risikobeurteilung
Gesamtheit des Verfahrens, das RISIKOANALYSE und RISIKOBEWERTUNG umfasst
[ISO/IEC Guide 51:1999, Definition 3.12]

2.16 Risikokontrolle
Prozess, durch den Entscheidungen herbeigeführt werden und Schutzmaßnahmen implementiert werden, um Risiken zu reduzieren oder um sie in festgelegten Grenzen zu halten

2.17 Risikobewertung
Beurteilung auf der Grundlage einer RISIKOANALYSE, ob auf der Basis der von der Gesellschaft anerkannten Werte ein vertretbares RISIKO in einem gegebenen Zusammenhang erreicht worden ist
ANMERKUNG Auf der Grundlage von ISO/IEC Guide 51:1999, Definition 3.11 und 3.7.

2.18 Risikomanagement
systematische Anwendung von Managementgrundsätzen, VERFAHREN und Praktiken auf die Analyse, Bewertung und Kontrolle von RISIKEN

2.19 Risikomanagement-Akte
Zusammenstellung von AUFZEICHNUNGEN und sonstigen Dokumenten, die durch den Risikomanagement-Prozess erzeugt werden und nicht notwendigerweise an einer Stelle sein müssen

2.20 Sicherheit
Freiheit von unvertretbaren RISIKEN
[ISO/IEC Guide 51:1999, DeÞnition 3.1]

2.21 Schweregrad
Maß der möglichen Folgen einer GEFÄHRDUNG

2.22 Verifizierung
Bestätigung aufgrund einer Untersuchung und durch Bereitstellung eines NACHWEISES, dass festgelegte Forderungen erfüllt worden sind
ANMERKUNG Im Design bezieht sich die VERIFIZIERUNG auf den PROZESS der Untersuchung des Ergebnisses einer gegebenen Tätigkeit, durch die die Konformität mit der festgelegten Anforderung für diese Tätigkeit festgestellt wird.
(ISO 8402:1994, Definition 2.17)

C. Definitionen gemäß IFIP WG 10.4 - Dependability tree (Übersetzung ins Deutsche durch Voges et al.) /Laprie1992, Avizienis2001/

1 Dependability (Zuverlässigkeit)
Dependability of a computing system is the ability to deliver service that can justifiably be trusted

1.1 Impairments (Beeinträchtigungen)
- **1.1.1 Faults (Fehlerursachen)**
- **1.1.2 Errors (Fehlzustände)**
- **1.1.3 Failures (Ausfälle)**

A system **failure** is an event that occurs when the delivered service deviates from correct service. A failure is thus a transition from correct service to **incorrect service**, i.e., to not implementing the system function. The delivery of incorrect service is a system **outage**.

1.2 Means (Mittel)
- 1.2.1 Procurements (Verfahren)
  - **1.2.1.1 Fault prevention (Fehlerverhinderung)**
  - **1.2.1.1 Fault tolerance (Fehlertoleranz)**
- 1.2.2 Validation (Validation)
  - **1.2.2.1 Fault removal (Fehlerbeseitigung)**
  - **1.2.2.2 Fault forecasting (Fehlervorhersage)**

1.3 Attributes (Kenngrößen)
- **1.3.1 Availability (Verfügbarkeit)**
- **1.3.2 Reliability (Funktionsfähigkeit)**
- **1.3.3 Safety (Sicherheit)**
- **1.3.4 Security (Vertraulichkeit)**
  the absence of unauthorized access to, or handling of, system state
  - **1.3.4.1 Confidentiality**
    the prevention of the unauthorized disclosure of information
  - **1.3.4.2 Integrity (Integrität)**
    the prevention of the unauthorized amendment or deletion of information
  - **1.3.4.3 Availability (Verfügbarkeit)**
    the prevention of the unauthorized withholding of information
- **1.3.5 Maintainability (Instandhaltbarkeit)**

D. Definitionen gemäß DIN 40041 /DIN1990/

1.4 Zuverlässigkeit (dependability)
Beschaffenheit einer Einheit bezüglich ihrer Eignung, während oder nach vorgegebenen Zeitspannen bei vorgegebenen Anwendungsbedingungen die Zuverlässigkeitsanforderungen zu erfüllen.

2.1.2 Funktionsfähigkeit (reliability)

Eignung einer Einheit, eine geforderte Funktion unter vorgegebenen Anwendungsbedingungen zu erfüllen.

2.1.4 Fehler (nonconformity)
Nichterfüllung einer Forderung

2.2.4 Ausfall (failure)
Beendigung der Funktionsfähigkeit einer materiellen Einheit im Rahmen der zugelassenen Beanspruchung.

E. Definitionen gemäß DIN 9000 /DIN2000/

3.5.3 Zuverlässigkeit (dependability)
Zusammenfassender Ausdruck zur Beschreibung der Verfügbarkeit und ihrer Einflussfaktoren Funktionsfähigkeit, Instandhaltbarkeit und Instandhaltungsbereitschaft
ANMERKUNG Zuverlässigkeit wird nur für allgemeine Beschreibungen in nichtquantitativem Sinn benutzt. [IEC 60050-191:1990]

3.8.4 Verifizierung (verification)
Bestätigung durch Bereitstellung eines objektiven Nachweises (3.8.1), dass festgelegte Anforderungen (3.1.2) erfüllt worden sind
ANMERKUNG 1 Die Benennung „verifiziert“ wird zur Bezeichnung des entsprechenden Status verwendet.

3.8.5 Validierung (validation)
Bestätigung durch Bereitstellung eines objektiven Nachweises (3.8.1), dass die Anforderungen (3.1.2) für einen spezifischen beabsichtigten Gebrauch oder eine spezifische beabsichtigte Anwendung erfüllt worden sind
ANMERKUNG 1 Die Benennung „validiert“ wird zur Bezeichnung des entsprechenden Status verwendet.
ANMERKUNG 2 Die Anwendungsbedingungen für Validierung können echt oder simuliert sein.

F. Definitionen gemäß IEV /IEV2001/

191-02-03 Zuverlässigkeit
zusammenfassender Ausdruck zur Beschreibung der *Verfügbarkeit* und ihrer Einflussfaktoren *Funktionsfähigkeit*, *Instandhaltbarkeit* und *Instandhaltungsbereitschaft*
ANMERKUNG: Zuverlässigkeit wird nur für allgemeine Beschreibungen in nichtquantitativem Sinne benutzt.

dependability
the collective term used to describe the availability performance and its influencing factors: reliability performance, maintainability performance and maintenance support performance
NOTE: Dependability is used only for general descriptions in non-quantitative terms.

191-05-25 menschliches Versagen (menschliches) Fehlverhalten
Handlung eines Menschen, die zu einem unerwünschten Ergebnis führt

mistake human error
a human action that produces an unintended result

G. Definitionen gemäß VDE 31000 /VDE1987/

2.1 Schaden
Schaden ist ein Nachteil durch Verletzung von Rechtsgütern auf Grund eines bestimmten technischen Vorganges oder Zustandes.

2.2 Risiko
Das Risiko, das mit einem bestimmten technischen Vorgang oder Zustand verbunden ist, wird zusammenfassend durch eine Wahrscheinlichkeitsaussage beschrieben, die die zu erwartende Häufigkeit des Eintritts eines zum Schaden führenden Ereignisses und das beim Ereigniseintritt zu erwartende Schadensausmaß berücksichtigt.

2.3 Grenzrisiko

Grenzrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes. Im allgemeinen lässt sich das Grenzrisiko nicht quantitativ erfassen.

2.4 Gefahr

Gefahr ist eine Sachlage, bei der das Risiko größer als das Grenzrisiko ist.

2.5 Sicherheit

Sicherheit ist eine Sachlage, bei der das Risiko nicht größer als das Grenzrisiko ist.

2.7 Schutz

Schutz ist die Verringerung des Risikos durch Maßnahmen, die entweder die Eintrittshäufigkeit oder das Ausmaß des Schadens oder beide einschränken.

X. Referenzen

/Avizienis2001/ Algirdas Avizienis, Jean-Claude Laprie, Brian Randell: Fundamental Concepts of Dependability. UCLA CSD Report no. 010028, 2001.

/DIN1990/ DIN 40041: 1990-12: Zuverlässigkeit – Begriffe. Beuth Verlag Berlin, 1990.

/DIN2000/ DIN EN ISO 9000:2000-12: Qualitätsmanagementsysteme – Grundlagen und Begriffe. Beuth Verlag Berlin, 2000.

/DIN2001/ DIN EN ISO 14971: 2001-03: Medizinprodukte – Anwendung des Risikomanagements auf Medizinprodukte. Beuth Verlag Berlin, 2001.

/DIN2002/ DIN EN 61508-4 (VDE 0803 Teil 4): 2002-08,: Funktionale Sicherheit elektrischer/elektronischer/programmierbar elektronischer sicherheitsbezogener Systeme – Teil 4: Begriffe und Abkürzungen. Beuth Verlag Berlin 2002.

/IEV2001/ Internationales Elektrotechnisches Wörterbuch. Beuth Verlag Berlin 2001.

/Laprie1992/ J. C. Laprie (ed.): Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese. Springer-Verlag Wien, 1992.

/VDE1987/ DIN VDE 31000 Teil 2:1987-12: Allgemeine Leitsätze für das sicherheitsgerechte Gestalten technischer Erzeugnisse – Begriffe der Sicherheitstechnik – Grundbegriffe. Beuth Verlag Berlin 1987.