Technische Sicherheit und Informationssicherheit

Unterschiede und Gemeinsamkeiten

**Felix Freiling · Rüdiger Grimm
Karl-Erwin Großpietsch
Hubert B. Keller · Jürgen Mottok
Isabel Münch · Kai Rannenberg
Francesca Saglietti**

Einführung

Unsere Gesellschaft hängt in umfassendem Maße vom zuverlässigen Funktionieren technischer Systeme und vom jederzeit möglichen Zugriff auf authentische und korrekte Informationen ab. Innerhalb dieser technischen Systeme spielen informationsspeichernde bzw. -verarbeitende Systeme eine immer größere Rolle; in einzelnen Branchen tragen sie mittlerweile über 50 % zur Wertschöpfung bei [1]. Diese Systeme, egal wo sie eingesetzt werden (z. B. in Rechenzentren, Banken, Autos usw.) sollen im Folgenden als *IT-Systeme* (kurz für: informationstechnische Systeme) bezeichnet werden. Durch ihre Funktion können sich technische Systeme in allen Lebensbereichen und auf alle vorstellbaren *Werte* auswirken, die sämtliche für Nutzer bedeutsame Aspekte umfassen, etwa menschliches Leben, Gesundheit und Unversehrtheit, Vermögen, Wissen, Gegenstände und persönliche Daten beteiligter ebenso wie nur mittelbar beteiligter Personen.

Im Allgemeinen muss man davon ausgehen, dass technische Systeme nicht immer fehlerlos sind und arbeiten, sondern dass sie von Beginn an bestehende oder erst mit der Zeit auftretende *Schwachstellen* enthalten. Schwachstellen können selbst bei bestimmungsgemäßem Gebrauch eines technischen Systems zu Fehlfunktionen führen, durch die Personen, Umwelt, Infrastruktur oder Daten geschädigt werden. Erst recht kann die funktional falsch verstandene oder grundsätzlich unsachgemäße Benutzung technischer, auch korrekt funktionierender Systeme die oben genannten Werte beeinträchtigen. Die vielfältigen Probleme und Aspekte bezüglich der Sicherung von IT-Systemen gegen derartige Effekte gewinnen zunehmend an Bedeutung.

Im Arbeitskreis „Begriffsbildung" des GI-Fachbereichs „Sicherheit" ist in den letzten Jahren in intensiven Diskussionen versucht worden, Grundbegriffe zur Charakterisierung dieses Problembereichs, die in der Fachöffentlichkeit mit

DOI 10.1007/s00287-013-0748-2

Felix Freiling
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)
Informatik 1 (IT-Sicherheitsinfrastrukturen)
Martensstr. 3
91058 Erlangen

Rüdiger Grimm
Universität Koblenz-Landau, IT-Risk-Management
Universitätsstr. 1
56070 Koblenz

Karl-Erwin Großpietsch
Moselstr. 6
53757 Sankt Augustin
E-Mail: karl-erwin.grosspietsch@online.de

Hubert B. Keller
Karlsruhe Institute of Technology (KIT)
Institut für Angewandte Informatik (IAI)
Hermann-von-Helmholtz-Platz 1
76344 Eggenstein-Leopoldshafen

Jürgen Mottok
Ostbayerische Technische Hochschule Regensburg
(OTH Regensburg)
Laboratory for Safe and Secure Systems (LaS^3)
Seybothstraße 2
93025 Regensburg

Isabel Münch
Bundesamt für Sicherheit in der Informationstechnik (BSI)
Cyber-Security
Godesberger Allee 185–189
53175 Bonn

Kai Rannenberg
Johann Wolfgang Goethe-Universität Frankfurt
Deutsche Telekom Stiftungsprofessur für Mobile
Business & Multilateral Security
Grüneburgplatz 1
60629 Frankfurt/Main

Francesca Saglietti
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)
Informatik 11 (Software Engineering)
Martensstr. 3
91058 Erlangen

teilweise divergierender Bedeutung benutzt wurden, präziser zu fassen. Als Resultat dieser Arbeiten wird in der vorliegenden Veröffentlichung auf die Bedeutung solcher unterschiedlicher, umgangssprachlich oftmals synonym gebrauchter Begriffe eingegangen, die nach Auffassung der Autoren einer differenzierten Betrachtung bedürfen. Die Arbeit ist wie folgt aufgebaut: Abschnitt „Grundbegriffe“ beschreibt einige Grundbegriffe aus dem Unfallwesen. Dann wird in Abschnitt „Sicherheitskonzepte“ eine Reihe von Definitionen zur genaueren Charakterisierung des Begriffs „Sicherheit“ vorgestellt. Danach diskutiert Abschnitt „Sicherheit von IT-Systemen einschließlich ihrer Umgebung“ die Übertragung dieser Notation auf IT-Systeme. Abschnitt „Die Sicherheitsterminologie im englisch beeinflussten Sprachgebrauch: Safety vs. Security und ihre terminologischen Unterfütterungen“ bringt einen Überblick über die verschiedenen Interpretationen der Begriffe „Safety“ und „Security“. Abschließend werden in Abschnitt „Technische Sicherheit und Informationssicherheit“ die Begriffe „Technische Sicherheit“ und „Informationssicherheit“ behandelt.

Grundbegriffe

Bedrohung, Schwachstelle, Gefährdung

Eine *Bedrohung* (engl. *threat*) ist eine Klasse potenzieller Ereignisse, durch deren Eintreten ein Schaden bewirkt werden kann. Der Schaden kann sich durch Beeinträchtigung der menschlichen Gesundheit oder der Umwelt bzw. durch Werteverluste materieller Natur (Vermögen, Wertgegenstände) oder immaterieller Natur (Vertraulichkeit, Information) äußern. Bedrohungen können durch höhere Gewalt, organisatorische Mängel, menschliche Fehlhandlungen, technisches Versagen oder vorsätzliche Handlungen bedingt sein. Eine Bedrohung wird erst durch das Vorhandensein einer oder mehrerer entsprechender Schwachstellen (engl. *vulnerabilities)*, etwa einer fehlenden Absicherung, zur *Gefährdung* (engl. *hazard*).

Eine Gefährdung besteht demnach im Falle der Anwesenheit einer Bedrohung bei gleichzeitigem Vorhandensein einer oder mehrerer Schwachstellen. Bei tatsächlichem Eintreten eines Bedrohungsereignisses (Angriff oder Ausfall/Störung/Versagen) kann die Gefährdung zu einem *Vorfall* (engl. *incident*) führen; tritt als Resultat ein Schaden auf, so

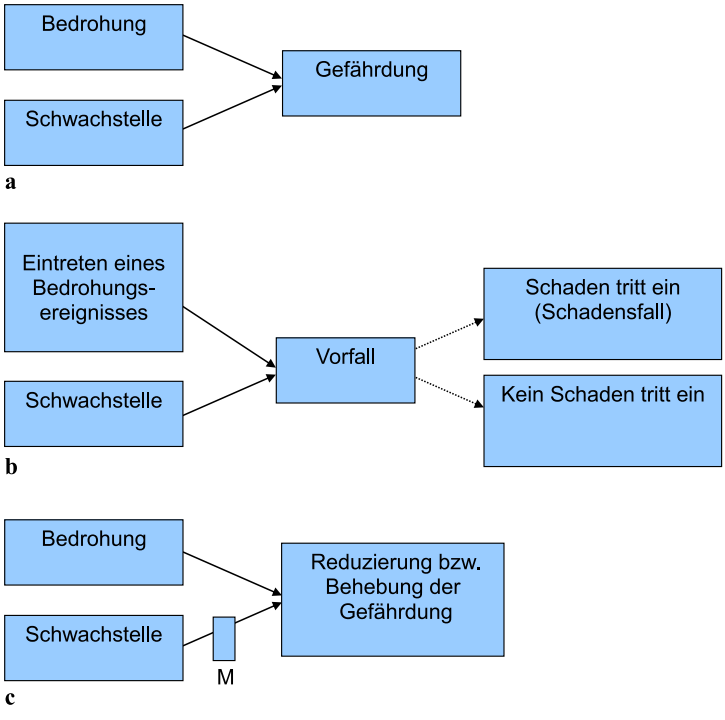

Abb. 1 a) Zusammentreffen von Bedrohung und Schwachstelle führt zu Gefährdung. b) Zusammentreffen des Eintretens eines Bedrohungsereignisses mit einer Schwachstelle führt zu einem Vorfall, eventuell mit Schaden verbunden. c) Spezifische Maßnahmen M zur Eingrenzung, Kompensation oder Eliminierung der Schwachstelle führen zur Reduzierung bzw. Behebung der Gefährdung

spricht man von einem *Schadensfall* (engl. a*ccident*). Ist ein solcher Schadensfall das Resultat böswilliger Planung, so spricht man von einem *Angriff* (engl. *attack*), andernfalls, je nach Schwere des Schadens, von Panne, Unfall, Havarie (letzteres z. B. bei Schiffen und Reaktoren) oder Unglück.

Durch geeignete Gegenmaßnahmen können Schwachstellen kompensiert oder zumindest eingegrenzt, in einigen Fällen sogar eliminiert werden, sodass dadurch das von Bedrohungen ausgehende Gefährdungspotenzial reduziert bzw. annulliert werden kann. Alle auf einer Autobahn fahrenden Verkehrsteilnehmer sind beispielsweise prinzipiell durch potenzielle Raser bedroht, selbst im Falle, dass gerade keiner vorhanden ist. Der Unglückliche jedoch, der einem konkreten Raser begegnet, wird von diesem gefährdet und möglicherweise auch geschädigt, wenn sein Fahrzeug nicht stabil genug ist, um einen Zusammenstoß abzufedern. Ein Panzerfahrer allerdings wird von einem Raser nicht gefährdet.

Der Zusammenhang zwischen den hier eingeführten Grundbegriffen ist in Abb. 1 zusammengefasst.

Risiko

Zwecks qualitativer bzw. quantitativer Bewertung von Gefährdungen wird das *Risiko* (engl. *risk*) durch Berücksichtigung folgender Aspekte ermittelt:

- Funktionen, Objekte, Werte bzw. Menschen, auf die sich die jeweilige Gefährdung auswirken kann;
- Eintrittswahrscheinlichkeit der betrachteten Gefährdung;
- Art und Umfang potenzieller Schäden infolge der betrachteten Gefährdung.

In der allgemein benutzten quantitativen Begriffsbestimmung wird das Risiko als Produkt aus der Eintrittswahrscheinlichkeit eines Schadensfalls und der daraus zu erwartenden Schadenshöhe definiert:

$$\text{Risiko} = \text{Schadenseintrittswahrscheinlichkeit} \times \text{Schadenshöhe}\,.$$

Allgemein wird die Größe des Risikos in Bezug gesetzt zu einem vorgegebenen Schwellwert, dem sog. *tolerierbaren Risiko* R_t, d. h. das Risiko wird als akzeptabel betrachtet, wenn es $\leq R_t$ ist, andernfalls ist es nicht akzeptabel. In manchen Fällen werden zusätzliche Maßnahmen getroffen, um die Größe des Risikos erheblich, z. B. um eine oder mehrere Größenordnungen zu reduzieren. Bei vielen technischen Systemen versucht man dies z. B. dadurch zu erreichen, dass für bestimmte Betriebsparameter anstelle eines grundsätzlich technisch möglichen Parameterwerts t_m ein weit unkritischerer Wert t_u benutzt wird. Der Absolutbetrag der Differenz beider Werte $|t_m - t_u|$ wird auch als *Sicherheitsabstand* bezeichnet. So wird ein Lastenaufzug, dessen Seil eine Tonne Last aushält, nur für 100 kg freigegeben, die Last also um den Faktor 10 reduziert.

Die oben angegebene Formel erlaubt, auch deterministisch eintretende Schadensfälle (garantiert eintretende Schadensfälle, ausgedrückt durch die zugeordnete Eintrittswahrscheinlichkeit $W = 1$ bzw. (aufgrund spezifischer Bedingungen oder Maßnahmen) unmöglich eintretende Schadensfälle, letztere ausgedrückt durch $W = 0$), mit zu beschreiben.

Hinsichtlich einer qualitativen Risikobewertung wird auf DIN 19250 [10] verwiesen.

Eine weitere Definition des Begriffs „Risiko“ erfolgt im ISO Guide 73:2009 („risk“ = „effect of uncertainty on objectives“ [31]).

Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ also bereits eine Bewertung, entweder des berechneten Schadensszenarios (probabilistisch) oder des gesicherten Abstands zu einer realisierbaren Gefährdung (deterministisch) im jeweils vorliegenden Fall.

Die Nutzung technischer Systeme ist stets mit Risiken verbunden; dabei werden Gefährdungen bewusst oder unbewusst in Kauf genommen, falls der angestrebte Nutzen nicht anders zu erzielen ist. Risiko-Wahrnehmung und Risiko-Akzeptanz sind individuell und kulturell geprägt, somit auch zeitlichen Veränderungen unterworfen (siehe z. B. [27]).

Die individuelle Akzeptanzschwelle kann u. U. auch dazu verleiten, seltene Gefährdungen mit schwerwiegenden Folgen zu akzeptieren, etwa weil

- das Risiko grundsätzlich *unbekannt* ist,
- das Risiko aufgrund fehlender Wahrnehmung *unterschätzt* wird („mir wird schon nichts passieren“),
- keine realistische *Alternative* besteht (z. B. Leben in einem Erdbebengebiet oder beruflich bedingtes, häufiges Autofahren),
- das Risiko durch den in Aussicht gestellten *Nutzen* überkompensiert wird.

In Abhängigkeit vom jeweiligen Systemeinsatz können also bestimmte Risiken als tolerierbar betrachtet werden, andere nicht. Beispielsweise mögen beim Autoverkehr gelegentliche Blechschäden tolerierbar sein, Personenschäden (selbst in seltenen Fällen) hingegen nicht, wobei das letztere Risiko häufig unterschätzt wird.

Aufgrund der Risikobewertung ergeben sich verschiedene Handlungsalternativen zum Umgang mit Risiken:

- *Risiko-Vermeidung* (engl. *risk avoidance*): Prozesse bzw. Systeme werden derart ausgelegt, dass das Eintreten vorgegebener, folgenschwerer Gefährdungen gezielt ausgeschlossen oder unter das tolerierbare Risiko gesenkt werden kann.
- *Risiko-Reduktion* (engl. *risk reduction*, auch *risk modification*): Durch geeignete Maßnahmen (z. B. Beherrschungsmechanismen) wird vorgegebenen, folgenschweren Gefährdungen entgegengewirkt.
- *Risiko-Transfer* (engl. *risk transfer*, auch *risk sharing*): Das bestehende Risiko wird anderweitig übertragen, zum Beispiel durch Abschluss eines Versicherungsvertrags oder durch Outsourcing.
- *Risiko-Übernahme* (engl. *risk retention*): Aufgrund der Risikobewertung sowie einer Kosten-Nutzen-Analyse wird die Möglichkeit des Eintretens potenzieller Gefährdungen akzeptiert.

Kombinationen obiger Formen können ebenfalls vorliegen.

Sicherheitskonzepte

Zur Bezeichnung der Abwesenheit bzw. Begrenztheit signifikanter Gefährdungen wird der Begriff *Sicherheit* verwendet. Dieser kann in der deutschen Sprache darüber hinaus ein sehr breites Spektrum möglicher Interpretationen annehmen, einschließlich folgender Bedeutungen:

- *Gewissheit* über die Korrektheit einer Aussage, also Sicherheit im Sinne der Zweifellosigkeit (engl. *doubtlessness, certainty*);
- *Grad des Vertrauens* in die Korrektheit einer Aussage, also Sicherheit im Sinne der Aussagesicherheit (engl. *confidence level*); dieser Grad kann prozentual gemessen werden und stimmt im Sinne des juristischen Begriffs „mit an Sicherheit grenzender Wahrscheinlichkeit“ mit oben genannter Gewissheit überein.
- *zu hinterlegendes Pfand bzw. zu erklärende Bürgschaft*, also Sicherheit im Sinne der Gewährleistung eines Gegenwertes im Falle des Eintretens eines Verlustes (engl. *guarantee*).

Selbst in Bezug auf das Vorhandensein von Gefährdungen kann der Begriff Sicherheit in Abhängigkeit von den zugrundeliegenden normativen Regelungen unterschiedliche Bedeutungen annehmen. Er kann hinweisen auf:

- eine Abwesenheit von Gefährdungen für den Fall, dass Schäden nicht oder in nicht signifikantem Umfang auftreten können (siehe ISO/IEC 27000 [15]); dies entspricht der umgangssprachlichen Bedeutung des Begriffs Sicherheit („sicher wie in Abrahams Schoß“ als deterministische Betrachtung bei gesichertem Kenntnisstand) und
- eine angemessene Seltenheit von Gefährdungen für den Fall, dass im Sinne eines begrenzten, *tolerierbaren Risikos* signifikante Schadensfälle nur bei entsprechend geringer Eintrittswahrscheinlichkeit möglich sind (siehe IEC 61508 [14] als probabilistische Betrachtung).

In dieser Arbeit soll nachfolgend eine Terminologie vorgeschlagen werden, die eine begriffliche Unterscheidung zwischen diesen Fällen ermöglicht.

Ein Beispiel einer klassischen Ingenieurdisziplin, die im Laufe von Jahrhunderten einen hohen Sicherheitsstandard erreicht hat, ist das Bauwesen. Für Gebäude lassen sich i. A. Häufigkeit und Schwere von durch Materialveränderungen (etwa infolge von Alterung, Belastung, Feuchtigkeit) bewirkten Schadensfällen adäquat niedrig halten; dabei wird natürlich vorausgesetzt, dass durch regelmäßige Wartungsmaßnahmen das Aufschaukeln von Kleinschäden zu größeren, nicht mehr beherrschbaren Schäden ausgeschlossen werden kann. So können i. A. jahrhundertealte Kathedralen gefahrenfrei betreten werden; selbst für Erdbeben beschränkter Stärke kann heutzutage die Gebäudestabilität garantiert werden. Der Grund hierfür ist, dass das durch Materialfestigkeit und Schwingungsverhalten bestimmte Stabilitätsverhalten quantitativ erfassbar und analysierbar ist; insbesondere kann dadurch mittels geeigneter Auslegung der Gebäudekonstruktion (etwa durch Verwendung massiver Materialredundanz) auch Stabilität gegenüber Fremdeinwirkungen wie Erdbeben bzw. Kollisionen mit Fahrzeugen oder entwurzelten Bäumen gewähr-

leistet werden. Der Einsturz des Kölner Stadtarchivs 2009 bietet hierzu kein Gegenbeispiel, da er offenbar durch hochriskante Baumaßnahmen ausgelöst wurde, die zu inakzeptablen Veränderungen der tragenden Bodenschichten führten.

Das Beispiel zeigt, dass zwar absolute Sicherheit gegen alle beliebigen Bedrohungen (einschließlich Naturkatastrophen u. a.) grundsätzlich nicht garantiert werden kann, dass dies aber für bestimmte konkrete Klassen von Gefährdungsprofilen (Schwachstellen und Bedrohungen) möglich ist. Eine solche Sicherheitsgarantie kann allerdings nur erfolgen, wenn die zugrundeliegenden Naturgesetze, ggf. in Verbindung mit nachweisbar exakten organisatorischen Maßnahmen, das Auftreten von Gefährdungen über einen vorgegebenen Schadensumfang zwingend ausschließen. In diesem Fall wird das System als *inhärent sicher* bezüglich der betrachteten Gefährdungsart bezeichnet.

Für komplexe technische Systeme, etwa elektronisch und digital arbeitende Systeme, sind derartige Sicherheitsgarantien kaum zu erbringen. Dies ist dadurch bedingt, dass bereits kleinste Fehler im System zu signifikanten Abweichungen in seinem Verhalten führen können. Fehler können während des Systemeinsatzes z. B. durch physikalisch bedingte Komponentenausfälle (wie etwa ausgefallene Transistoren) auftreten oder von Anfang an im System vorhanden sein (wie etwa Programm- oder Datenfehler).

Für solche Systeme müssen einerseits komplexe, die möglichen Schadensursachen differenziert betrachtende Zuverlässigkeitsanalysen, andererseits ergänzende, u. U. umfangreiche Schutzmaßnahmen konzipiert und umgesetzt werden. Falls diese Schutzmaßnahmen nachweislich immer zur Beherrschung vorgegebener Gefährdungsklassen führen, so kann das System als *aufgrund von Schutzmaßnahmen sicher* betrachtet werden und wird im Folgenden in Bezug auf die zugrundeliegende Gefährdungsklasse als *schutzbedingt sicher* bezeichnet werden.

Systeme, die *inhärent* oder *schutzbedingt sicher* sind, fassen wir unter dem Oberbegriff *deterministisch sicher* zusammen. Systeme, die in Bezug auf eine Gefährdungsklasse zwar nicht deterministisch sicher sind, bei denen aber zumindest eine risikoadäquate Schadensseltenheit nachgewiesen werden kann, werden als *probabilistisch sicher* bezeichnet. Diese Betrachtung harmoniert mit der in IEC 61508 [14] vorgenommenen Definition von Sicherheit als „Abwesenheit nicht-tolerierbarer Risiken", wodurch gravierende Schäden nicht ausgeschlossen werden, solange sie mit hinreichend niedriger Wahrscheinlichkeit auftreten (Beispiel: Ausfall aller Triebwerke beim Flug über den Atlantik). Probabilistisch sichere Systeme lassen sich dahingehend weiter unterteilen, ob der Einfluss von Schwachstellen langsam, stetig wächst (Kontinuumsprinzip) oder aber sich sprunghaft, unstetig ändert (s. Abb. 2).

Stetig sich ändernde Systeme sind z. B. die Bremsanlagen eines Fahrzeugs, welche durch die Benutzung allmählich verschleißen und sich im normalen Betriebsmodus zwar immer um einen gewissen Grad in ihrem Zustand verschlechtern, aber in aller Regel nicht schlagartig ausfallen (Anmerkung: Dem auch beim Kontinuumsprinzip möglichen schlagartigen, nicht durch stetigen Verschleiß resultierenden Ausfall einer einzelnen Bremsanlage wird in der heutigen Automobiltechnik durch das redundant aufgebaute Diagonal-Zweikreisbremssystem begegnet).

Software allerdings kann durch die Änderung der Art ihrer Benutzung, trotz vorherigen fehlerfreien Funktionierens, in der neuen Benutzungsart schlagartig versagen. Durch die geänderte Nutzung

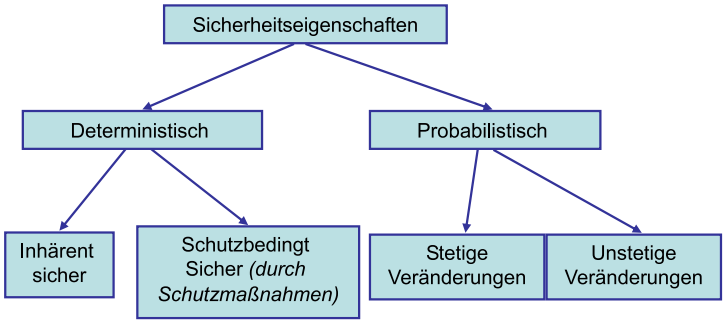

Abb. 2 Sicherheitseigenschaften bezüglich gegebener Gefährdungsklasse

können z. B. vorher nicht verwendete Ablaufstrukturen aktiv werden, welche durch eine schon immer vorhandene Schwachstelle (Programmfehler) sofort zu einem Fehlverhalten (Absturz usw.) führen können.

Fehler in der Software sind in der Regel immer vorhanden. Bestimmte Eingangsvoraussetzungen führen dann zu einer Fehleraktivierung, wobei die Eintrittswahrscheinlichkeit dieser Voraussetzungen im Allgemeinen nicht bekannt ist (siehe hierzu [28]). Ein vollständiger Test von Software unter allen zugelassenen Betriebsprofilen kann aufgrund der resultierenden Testkomplexität i. A. nicht durchgeführt werden [29]. Der Reifegrad, den die Software für ein bestimmtes Benutzungsprofil erreicht hat, kann also bei einem gänzlich anderen Benutzungsprofil nicht erwartet werden.

Sicherheit von IT-Systemen einschließlich ihrer Umgebung

Ein IT-System besteht funktional aus folgenden Komponenten:

- den *Hardwareplattform(en)*: Prozessor(en), Arbeitsspeicher, Hintergrundspeicher, Eingabe/Ausgabe-Geräte einschließlich Sensoren und Aktoren sowie sonstige Kommunikationskomponenten (wie Busse und systeminterne Netzwerke) und
- den *Softwarekomponenten*: System- und Anwendungsprogramme einschließlich ihrer Daten.

Dem IT-System ist bestimmungsgemäß eine Umgebung, mit der Wechselwirkungen möglich sind, zugehörig. Zur *engeren Systemumgebung (Kernumgebung)* gehören:

- die *Systemverwaltung* (ggf. auch Inbetriebnahme, Wartung) sowie
- die *direkte Umgebung* (z. B. Räumlichkeiten, in denen das System sich befindet, oder die direkte Umgebung eines Einbauortes, bei eingebetteten Systemen die damit verbundene weitere Hardware).

Beispielsweise muss ein Serverraum vor Stromausfall, Unwettereinwirkungen, Sabotage geschützt werden; dies ist etwa erzielbar durch Zutrittskontrollsysteme, Brandschutz u. a.

Zur darüber hinausgehenden *peripheren Umgebung* eines IT-Systems zählen etwa weitere IT-Systeme (z. B. Server), mit denen das IT-System über Netze kooperiert; sie lässt sich wie folgt gliedern:

- die *beeinflussbare periphere Umgebung*, d. h. die periphere Umgebung, auf die externe technische, administrative oder sonstige Prozesse etwa durch Steuerung Einfluss nehmen können;
- die *beeinflussende periphere Umgebung*, d. h. die periphere Umgebung, die durch Sensormessung, aber auch durch exogene Gefährdungen wie etwa Stromausfall, Unwettereinwirkungen, Sabotage usw. auf das System Einfluss nehmen können; während der Entwurfsphase des IT-Systems gehören z. B. auch die Systemkonstrukteure hierzu.

Ein IT-System soll als (*inhärent, schutzbedingt, deterministisch* bzw. *probabilistisch*) *sicher* bezeichnet werden, wenn es sowohl in Bezug auf seine Komponenten als auch in Bezug auf seine bestimmungsgemäße Umgebung die entsprechenden, oben eingeführten Sicherheitseigenschaften erfüllt. Dabei muss der Nachweis auf dem aktuellen Erkenntnisstand (Stand der Technik und Stand der Wissenschaft) basieren. Damit sind sowohl die „Security"-Aspekte wie Vertraulichkeit, Integrität, Zugriffsfreiheit, Zurechenbarkeit etc. als auch die „Safety"-Aspekte wie hohe Zuverlässigkeit, Fehlersicherheit, Fehlertoleranz, sicherer Zustand usw. in Summe zu betrachten.

Im Unterschied zur *Sicherheit eines IT-Systems*, die alle oben genannten Schutzaspekte hinsichtlich des potenziellen Verhaltens des IT-Systems beinhaltet, werden heute üblicherweise mit der Kurzform *IT-Sicherheit* lediglich die datenbezogenen Schutzaspekte angesprochen. Diese terminologische Kollision erscheint unglücklich, nicht nur, weil sie zu Verwechslungen führen kann, sondern insbesondere deshalb, weil in heutigen Anwendungen eine getrennte Betrachtung des informationsverarbeitenden/informationsspeichernden Systems und seiner Umgebung unzweckmäßig, wenn nicht gar unmöglich ist.

Während der unterschiedlichen Phasen des Lebenszyklus eines IT-Systems kann sich das Gefährdungsprofil des IT-Systems ändern; beispielsweise unterscheiden sich i. A. die Gefährdungen (aufgrund phasenspezifischer Schwachstellen und Bedrohungen) in der *Entwicklungs-* oder *Produktionsphase* von denen in der *Betriebsphase*.

Die Sicherheitsanalyse muss diesen Änderungen Rechnung tragen. Darüber hinaus muss analysiert werden, inwieweit früh aufgetretene, nicht erkannte Schäden (etwa Analyse- oder *Produktionsfehler*) sich auf spätere Phasen auswirken können. Insbesondere ist zu berücksichtigen, dass sich Analyse- oder Produktionsfehler u. U. erst während des Systembetriebs, und auch dann meist nur in Abhängigkeit vom nutzerspezifischen Anforderungsprofil, manifestieren [23]).

Die Sicherheitsterminologie im englisch beeinflussten Sprachgebrauch: Safety vs. Security und ihre terminologischen Unterfütterungen

Als englische Äquivalente des deutschen Begriffs *Sicherheit* bieten sich die beiden Begriffe *Security* und *Safety* an. Beide beinhalten die Abwesenheit von Gefährdung, (engl. *freedom from danger*) und spiegeln in diesem Sinne nicht nur die reale, objektive Abwesenheit von Gefährdungen wider, sondern auch das subjektive Vertrauen des Systembenutzers hinsichtlich des bestehenden Schutzes vor folgenschweren Ereignissen.

Da sich zahlreiche internationale Forschungsgemeinschaften dieser beiden Begriffe mit (z. T. geringfügig) abweichenden Bedeutungen bedienen, lässt sich – trotz der in jüngster Zeit zunehmenden Bemühungen um Harmonisierung der Sichtweisen – eine eindeutige, allgemeingültige Definition der zwischen ihnen liegenden Demarkationslinie nicht erreichen.

Einerseits lässt sich feststellen, dass im Zusammenhang mit technisch und organisatorisch geprägten Systemen oft der Unterschied ursachenbezogen getroffen wird, indem

- *Security* oft mit der Sicherheit vor Angriffen bzw. Anschlägen gleichgestellt wird, was insbesondere die Existenz eines Angreifers voraussetzt, während
- *Safety* häufig die Sicherheit vor der Auswirkung unbeabsichtigter, etwa naturbedingter oder fehlerbedingter Gefährdungen, beinhaltet.

Andererseits wird auch im Hinblick auf die Art der gefährdeten Werte differenziert [18], nämlich der

- durch *Security-Maßnahmen* zu schützenden Daten und Informationen, sowie
- durch *Safety-Maßnahmen* zu schützenden materiellen Werte in der Systemumgebung (Menschen, Umwelt, Hardware, sonstige Infrastruktur) und im System selbst.

Im letzteren Fall umfasst *Security* oft drei Eigenschaften (in [6] als die drei Grundwerte der Informationssicherheit bezeichnet):

- *Informationsvertraulichkeit* (engl. *information confidentiality*): vertrauliche Informationen müssen vor unbefugter oder unbeabsichtigter Preisgabe geschützt werden,
- *Datenintegrität* (engl. *data integrity*): die Daten sind vollständig und unverändert bereitzustellen und
- *Verfügbarkeit* (engl. *availability*): dem Benutzer müssen Dienstleistungen, Funktionen eines IT-Systems oder auch Informationen zum geforderten Zeitpunkt zur Verfügung stehen.

Die drei Eigenschaften entsprechen im Wesentlichen der in den deutschen IT-Sicherheitskriterien (Grünbuch) [30] und den europäischen „Evaluation Criteria For IT Security“ (ITSEC) [8] verwendeten Begrifflichkeit. Diese Begriffswelt spiegelt auch den Definitionsansatz aus [2] wider, einer Weiterentwicklung des Definitionsansatzes von Laprie [16]. Tatsächlich geben diese drei Begriffe das wieder, was der Benutzer als sichere Benutzung von Daten erwartet, nämlich, dass das IT-System unmanipuliert zur Nutzung bereitsteht und dass Daten nicht unzulässig gelesen bzw. verändert werden können.

Ähnliche Varianten für den Begriff Security liefern [17]:

- *information security:* – the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability

bzw. ISO/IEC 27000 [15]:

- *information security* – preservation of confidentiality, integrity and availability of information.

In [24] wird moniert, dass die Bedrohung *Verlust der Verbindlichkeit* nicht berücksichtigt ist. Eine entsprechende Sicherheitseigenschaft *Accountability* (*Zurechenbarkeit*) findet sich auch in den ersten, US-amerikanischen, „Trusted Computer System Evaluation Criteria“ (Orange Book) [26] und den kanadischen IT-Sicherheitsevaluationskriterien [7].

Auch in [13] wurden für die Gesellschaft für Sicherheitswissenschaft die obigen drei *Security*-bezogenen Eigenschaften um zwei weitere Begriffe juristischer Natur erweitert, die von der Bundesregierung in den Jahren 2003/2004 im nationalen Sicherheitsplan bzw. IT-Sicherheitsplan übernommen wurden:

- *Verbindlichkeit* (engl. *liability, non-repudiability*) und
- *Rechtssicherheit* (engl. *legal certainty*).

Hierzu konsistent definiert [11] *Security* als die Eigenschaft eines funktionssicheren Systems, welches nur solche Systemzustände annehmen kann, die zu keinem unautorisierten Zugriff auf Systemressourcen und insbesondere auf Daten führen. Das entspricht der ursprünglichen Idee von [4] und [5], die diese Eigenschaft frühzeitig im „Basic Security Theorem" beschrieben haben. Andererseits erscheint in der gleichen Quelle [11] die Definition von *Safety* als die Eigenschaft eines Systems, wonach die realisierte Ist-Funktionalität der Komponenten mit der spezifizierten Soll-Funktionalität übereinstimmt. Dies ist nur dann mit den oben genannten risikobasierten Überlegungen kompatibel, falls vorausgesetzt werden kann, dass die spezifizierte Soll-Funktionalität im Hinblick auf die Sicherheit umfassend korrekt (berücksichtigt) ist, die Soll-Funktionalität also auch im Störungsfall erbracht wird (im Gegensatz zur Funktionsreduzierung bis hin zum sicheren Zustand ohne Funktionserbringung).

In [9] wurde eine „duale" Sicht auf die Sicherheit entwickelt, indem dort eine technische Sicht auf die Verlässlichkeit (*dependability*) von der menschlichen Sicht auf die Beherrschbarkeit (*controllability*) von IT-Systemen unterschieden wird. Dabei bezieht man sich ausdrücklich auf die in [19] eingeführte „Mehrseitige Sicherheit", die davon ausgeht, dass Sicherheit aus der gesamten Sicht verschiedener, oft sogar einander im Konflikt stehender Interessen betrachtet werden muss.

Schließlich gibt es auch Ansätze, die die beiden Begriffe *Safety* und *Security* im Hinblick auf die Art der eingreifenden Schutzmaßnahmen zu definieren, etwa in [18]:

- *Safety* als Zustand eines Systems, in dem Schutzmaßnahmen zur Vermeidung von Schäden wirksam sind und
- *Security* als Zustand eines Systems, in dem Maßnahmen zum Schutz der IT-Systeme wirksam sind

bzw. in [20] durch Betonung der entgegengerichteten Schutzwirkungen:

- *Safety* zum Schutz der Umgebung eines IT-Systems (einschließlich der Benutzer sowie aller im Einflussbereich sich aufhaltenden Menschen und Umweltelemente) vor Fehlverhalten des IT-Systems und
- *Security* zum Schutz des IT-Systems vor unerwünschtem Verhalten seiner Umgebung (sei dieses Verhalten durch Benutzerunerfahrenheit, höhere Gewalt oder kriminelle Angriffe bedingt).

In [3] wird aus Sicht der Entwicklung hochzuverlässiger Software ähnlich argumentiert und *Safety* als „the software must not harm the world" und *Security* als „the world must not harm the software" charakterisiert.

In [25] wird ein Ansatz vorgestellt, der versucht, ein vereinheitlichtes *Safety-Security*-Begriffsmodell auf der Basis des Begriffs *mishap* für die generalisierte Betrachtung von Schadensfällen sowohl im *Safety*- als auch im *Security*-Bereich aufzubauen.

Selbstverständlich müssen *Safety* und *Security* nicht notwendigerweise als binäre Konzepte begriffen werden, die entweder erfüllt oder nicht erfüllt sind; vielmehr lassen sich auch hier abgestufte Erfüllungsgrade als Maße einführen, wie in [12] vorgeschlagen:

- „*Safety* is the degree to which accidental harm is prevented, detected, and properly reacted to" und
- „*Security* is the degree to which malicious harm to a valuable asset is prevented, detected, and reacted to. Security is the quality factor that signifies the degree to which valuable assets are protected from significant threats posed by malicious attackers".

Technische Sicherheit und Informationssicherheit

Aus der Betrachtung der Struktur des IT-Systems in Abschnitt „Sicherheit von IT-Systemen einschließlich ihrer Umgebung" folgend, bieten sich zur Charakterisierung größerer Teilbereiche der Systemsicherheit zwei zentrale Unterbegriffe an, für die wir nach ausführlicher Untersuchung und vergleichender Bewertung der genannten Quellen folgende Terminologie vorschlagen:

– *Technische (oder funktionale) Sicherheit*:
  Freiheit bzw. Begrenztheit von Gefährdungen für das IT-System und für die Umgebung des IT-Systems im Sinne aller materiellen Objekte, auf die sich das Verhalten des IT-Systems auswirken kann.
– *Informationssicherheit*:
  Freiheit bzw. Begrenztheit von Gefährdungen für z. B. die *Vertraulichkeit* (engl. *confidentiality*), *Integrität* (engl. *integrity*), *Verfügbarkeit* (engl. *availability*) oder *Authentizität* (engl. *authenticity*) aller Informationen und Daten (einschließlich der Programme) in einem IT-System.

Wesentlichen Hintergrund dieser Unterscheidung bildet die Betrachtung der *initialen Schadensursache* (unabhängig von der Art des später eingetretenen Folgeschadens):

– Bei der *Technischen Sicherheit* ist die initiale Schadensursache das *Fehlverhalten einer oder mehrerer materieller Systemkomponenten*. Der Ort des Schadens ist das System (eine oder mehrere seiner Komponenten) einschließlich der bestimmungsgemäßen Umgebung des IT-Systems, d. h. der Umwelt, die Schaden nehmen kann, weil das IT-System falsch auf sie einwirkt. Je nach betrachteter Anwendung kann dabei eine Garantie der Schadensbegrenzung im Hinblick auf das System selbst oder auf dessen Umgebung (einschließlich Benutzer) im Vordergrund der Betrachtung stehen. Gefährdungen im Sinne der Technischen Sicherheit sind Ereignisse, die zu unerwünschtem, schädlichem Systemverhalten führen.
– Bei der *Informationssicherheit* liegt die initiale Schadensursache in *unzulässigen Operationen auf Informationen* (Daten inkl. Programminstruktionen bzw. die damit assoziierte Information). Der Ort des resultierenden primären Schadens ist der Informationsraum (Daten) des betrachteten Systems.

Ausgehend von der initialen Schadensursache ist zu beachten, dass sich einerseits Datenmanipulationen kritisch auf die Technische Sicherheit auswirken können (z. B. erfolgt durch falsche Daten ein inkorrekter Bremseingriff oder eine inkorrekte FPGA-Rekonfiguration und in Folge dann ein Fehlverhalten); andererseits kann sich das Fehlverhalten technischer Komponenten auf die Informationssicherheit kritisch auswirken (z. B. durch Beeinträchtigung der Verfügbarkeit bzw. der Integrität der Daten).

Hinsichtlich der Änderungen insgesamt lässt sich die gesamte Problematik mittels folgender Fallunterscheidung klassifizieren:

Verhaltensänderungen von Hardware können hervorgerufen werden durch

– *naturbedingte Ausfälle* (infolge Alterung, Verschleiß, elektromagnetische Strahlung usw.), bzw.
– *gezielte Eingriffe*, die sowohl nicht autorisierte, korrekt autorisierte als auch inkorrekte und dennoch autorisierte Handlungen reflektieren können.

Datenveränderungen können erfolgen aufgrund

– *physikalischer Einflüsse* (z. B. Bit-Kippen, Temperatur) bzw.
– *gezielter Änderungsbefehle*, wobei diese unautorisiert oder autorisiert sein können; in letzterem Fall kann es sich um zweckmäßige Änderungen, aber auch um autorisierte, obwohl inkorrekte Verhaltensweisen handeln (wie etwa die Pumpenabschaltung beim AKW Harrisburg 1979).

Als Konsequenz der allseitigen Auswirkungen ist bei heutigen Systemen eine klare Trennung zwischen beiden initialen Ursachenquellen praktisch nicht mehr möglich. Daher muss in Zukunft möglichst die gesamte *Sicherheit* des IT-Systems, die sowohl die Aspekte der Technischen Sicherheit als auch die Aspekte der Informationssicherheit umfasst, analysiert und angestrebt werden.

Im Hinblick auf die unterschiedlichen *Phasen des Systemlebenszyklus* (Entwicklung, Fertigung, Inbetriebnahme, Betrieb, Wartung, Entsorgung) ergibt sich zur Gewährleistung der Technischen Sicherheit sowie der Informationssicherheit ein Bedarf an konstruktiven Maßnahmen (Modularisierung, Redundanz, Diversität, Wahl von Auslegungsparametern) und an zugehörigen analytischen bzw. Simulations-Methoden zur Auslegung und Überprüfung dieser Maßnahmen. Bei der Systementwicklung müssen alle Wechselwirkungen beider Sicherheitsaspekte und ihre im Eintretensfall resultierenden Auswirkungen z. B. mittels Methoden wie FMEA (*failure mode and effects analysis*) oder SFTA (*software failure tree analysis*) analysiert und konstruktiv entsprechend den zu erreichenden Sicherheitsklassen beherrscht werden [21, 22]. Hinzu kommen entsprechende organisatorische Maßnahmen. Hierzu kann auch die Verweigerung

unzulässiger Benutzung gehören (z. B. Verhinderung des Einschaltens der Schubumkehr, solange das Flugzeug sich in der Luft befindet). Eine ausführliche Darstellung aller dieser Aspekte findet man in [27].

Zusammenfassung

Ziel dieser Arbeit war es, den Begriff der Sicherheit bei IT-Systemen und seine verschiedenen Aspekte genauer zu umreißen und auf elementare Aspekte zurückzuführen. Hierzu wurden zunächst einige Grundbegriffe eingeführt; darauf aufbauend wurde die unterschiedliche Verwendung des Begriffs Sicherheit sowohl in der Umgangssprache als auch bei der Charakterisierung und Analyse technischer Systeme diskutiert. Sicherheit bedeutet also zuerst die Risikoanalyse und nachfolgend die Art der Beherrschung bzw. des Umgangs damit. Als Konsequenz ergibt sich also eine abgestufte Klassifizierung des Sicherheitsbegriffs für IT-Systeme von inhärent sicher bis zu einer probabilistischen Bewertung der Sicherheitslage.

Der zentrale Ansatz zur weiteren begrifflichen Detaillierung der Definition von Sicherheit ist die *initiale Schadensursache* (Veränderung von Systemkomponenten oder Informationen) und der *Ort des Auftretens der Auswirkung* (System und Umgebung oder Informationsraum). Durch die enge gegenseitige Abhängigkeit der betrachteten Aspekte ist aber letztlich eine getrennte Betrachtung nicht möglich. Beide Aspekte sind also gemeinsam zu betrachten.

Zu den bisherigen Ausführungen über Sicherheit kommt der Mensch als weiterer Faktor hinzu. Bei komplexen Systemen spielt es naturgemäß auch eine Rolle, inwieweit die Benutzer Art und Zweck der Benutzung korrekt erfasst haben. Dies bedeutet in letzter Konsequenz, dass ein System in obigem Sinne sicher sein und dennoch gefährdend eingesetzt werden kann, falls es vom Benutzer, auch unwissentlich, missbraucht wird und keine Verriegelungsmechanismen dagegen vorhanden sind. Die *Beherrschbarkeit* (engl. *controllability*) des zu benutzenden Systems hängt also auch vom Systemverständnis des Benutzers ab. In Abhängigkeit von dem zur Nutzung einer Anwendung notwendigen Grad an Bedienungs-Kompetenz kann und soll die Beherrschbarkeit des IT-Systems durch robustere Auslegung der Mensch-Maschinen-Schnittstelle adäquat erhöht werden.

Erst wenn das System und seine Interaktionsschnittstellen als sicher bezeichnet werden können und dann auch die menschliche Interaktion mit der geplanten Verwendung des Systems hinreichend gesichert ist, kann von einem beherrschbaren System gesprochen werden. Eine sichere Beherrschbarkeit kann auf Basis der hier betrachteten technischen Sicherheit mit dem zur gefahrlosen Nutzung notwendigen Wissensstand seitens der Benutzer über das zu benutzende System erreicht werden.

Literatur

1. Abschlussbericht DFG-Schwerpunktprogramm 1040, Entwurf und Entwurfsmethodik eingebetteter Systeme, Wolfgang Rosenstiel, Universität Tübingen, BMW AG, 1997–2003
2. Avizienis A, Laprie JC, Randell B, Landwehr C (2004) Basic concepts and taxonomy of dependable and secure computing. IEEE Trans Dependable Secur Comput 1(1):11–33
3. Barnes J (2008) Safe and Secure Software – an invitation to Ada 2005. AdaCore, New York
4. Bell DE, LaPadula LJ (1973) Secure Computer Systems: Mathematical Foundations. MITRE Corporation
5. Bell DE, LaPadula LJ (1976) Secure Computer System: Unified Exposition and Multics Interpretation. MITRE Corporation. http://csrc.nist.gov/publications/history/bell76.pdf, letzter Zugriff: 13. November 2013
6. Bundesamt für Sicherheit in der Informationstechnik (2009) Leitfaden Informationssicherheit. Bundesamt für Sicherheit in der Informationstechnik, Bonn
7. Canadian System Security Centre (1993) The Canadian Trusted Computer Product Evaluation Criteria, Version 3.0e; January 1993, Communications Security Establishment, Government of Canada
8. Commission of the European Communities, (Informal) EC advisory group SOG-IS (1991) Information Technology Security Evaluation Criteria (ITSEC), Provisional Harmonised Criteria – Version 1.2; 28 June 1991; Office for Official Publications of the European Communities, Luxembourg. www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile, letzter Zugriff: 13. November 2013
9. Dierstein R (2004) Sicherheit in der Informationstechnik Informationssicherheit. Der Begriff der IT-Sicherheit und ihre Besonderheiten – Duale Sicherheit. Informatik-Spektrum 24(4):343–353; eine erweiterte Fassung gibt es als Arbeitsbericht der TU München unter dem Titel „IT-Sicherheit und ihre Besonderheiten – Duale Sicherheit", Januar 2008. http://www.lrr.in.tum.de/public/download/TeachingItSicherheitWS07DualeSicherheit, letzter Zugriff: 13. November 2013
10. Deutsche Elektrotechnische Kommission im DIN und VDE (Hrsg.) (1989) Vornorm DIN 19250 Grundlegende Sicherheitsbetrachtungen, Betrachtungen für MSR-Schutzeinrichtungen. Beuth, Berlin
11. Eckert E (2012) IT-Sicherheit, Konzepte – Verfahren – Protokolle, 7. Aufl. Oldenbourg, München
12. Firesmith DG (2003) Common Concepts Underlying Safety, Security, and Survivability Engineering, Technical Note, CMU/SEI-2003-TN-033. Carnegie Mellon University, Pittsburgh
13. Hauff H (1997) IT-Sicherheit – die massenmediale Sicht. 2. Cottbuser Risiko-Symposium. BTU, Cottbus
14. IEC 61508 Standard (1998) Functional safety of electrical/electronic/programmable electronic safety-related systems. Teil 1 bis 7. IEC
15. ISO/IEC 27000:2009 (2009) Information security management systems — Overview and vocabulary. http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip, letzter Zugriff: 13. November 2013
16. Laprie JC (1992) Dependability: Basic Concepts and Terminology in English, French, German, Italian and Japanese. Springer, Wien
17. NIST IR 7298 Rev. 2 (2013) Glossary of Key Information Security Terms. Richard Kissel, Editor, May 2013. http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf, letzter Zugriff: 13. November 2013
18. Pohl H (2004) Taxonomie und Modellbildung in der Informationssicherheit. Datenschutz und Datensicherheit 28(11):678–685

19. Rannenberg K, Pfitzmann A, Müller G (1996) Sicherheit, insbesondere mehrseitige IT-Sicherheit. Informationstechnik und Technische Informatik (it+ti) 38(4):5–10
20. Saglietti F (2006) Interaktion zwischen funktionaler Sicherheit und Datensicherheit, Sicherheit 2006: Sicherheit – Schutz und Zuverlässigkeit. Lecture Notes in Informatics, Gesellschaft für Informatik
21. Barbacci M, Klein MH, Longstaff TA, Weinstock CB (1995) Quality Attributes, Technical Report, CMU/SEI-95-TR-021, ESC-TR-95-021. December 1995
22. Barbacci MR, Klein MH, Weinstock CB (1997) Principles for Evaluating the Quality Attributes of a Software Architecture, Technical Report. CMU/SEI-96-TR-036, ESC-TR-96-136, May 1997
23. Söhnlein S, Saglietti F, Bitzer F, Meitner M, Baryschew S (2010) Software Reliability Assessment Based on the Evaluation of Operational Experience, Lecture Notes in Computer Science, Vol. LNCS 5987, Springer, New York
24. Stelzer D (1990) Kritik des Sicherheitsbegriffs im IT-Sicherheitsrahmenkonzept. Datenschutz Datensich (DuD) 14(10):501–506
25. Stoneburner G (2006) Toward a unified security/safety model. Comp 8:86–87
26. USA Department of Defense, Department of Defense Trusted Computer Security Evaluation Criteria (Orange Book) (1985) DoD 5200.28-STD
27. Eschenfelder D, Gelfort E, Graßmuck J, Keller H, Langenbach C, Lemiesz D, Otremba F, Pilz WD, Rath R, Schulz-Forberg B, Wilpert B (2010) Qualitätsmerkmal „Technische Sicherheit", Eine Denkschrift des Vereins Deutscher Ingenieure. Düsseldorf
28. Voges U (1998) Software-Diversität und ihr Beitrag zur Sicherheit. In: Keller HB (Hrsg) Entwicklung von Software-Systemen mit Ada. Ada-Deutschland Workshop Bremen, Wissenschaftliche Berichte des FZKA 6177, Forschungszentrum Karlsruhe
29. Watts SH (2008) The Software Quality Challenge, Software Eng. Institute, Crosstalk 6
30. Zentralstelle für Sicherheit in der Informationstechnik (1989) IT-Sicherheitskriterien – Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT) (Grünbuch). Bundesanzeiger-Verlag, Köln, 1. Fassung vom 11. Januar 1989, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itgruend_pdf.pdf;jsessionid=701A4BA7C7C41A00E2495C831A9E027C.2_cid294?__blob=publicationFile, letzter Zugriff: 13. November 2013
31. ISO (2009) ISO Guide 73:2009 – Risk management – Vocabulary, Section 1 „Terms relating to risk", Definition 1.1. ISO/TC 262, http://www.iso.org/iso/home/store/catalogue_tc/, letzter Zugriff: 11. November 2013