Ohne *Security* keine *Safety* in Kritischen Infrastrukturen — Begriffliche Trennung und Zusammenführung

Lars Fischer[1,2] and Michel Messerschmidt[2]

[1] *Carl-von-Ossietzky Universität Oldenburg*
[2] *AG KRITIS*

4. Mai 2020

Wenn es erst einmal brennt, dann bleibt keine Zeit mehr um Misverständnisse auszudiskutieren. Und auch vorher, wenn Systeme entwickelt und aufgebaut werden um die Infrastruktur unserer Gesellschaft zu bilden, ist es wesentlich, dass die Akteure miteinander Kommunizieren können. In diesem Artikel wollen wir die Unterscheidung der englischen Begriffe *Safety* und *Security* formulieren, was insbesondere deshalb wichtig ist, weil viele andere Sprachen beide Konzepte mit nur einem Wort beschreiben. Beide Konzepte formulieren aber unterschiedliche und häufig auch konkurrierende Ziele. Deshalb ist es wesentlich, diese Konzepte klar zu definieren und in der Arbeit zu unterscheiden. Im Folgenden geben wir deshalb eine Einführung und praktische Definitionen und zeigen beispielhaft das Konfliktpotential auf.

1 Kritische Infrastruktur

Das wesentliche Merkmal von Systemen, die unter dem Begriff *Kritische Infrastrukturen* gebündelt werden, ist die Notwendigkeit ihrer Funktionen für den Erhalt der Gesellschaft ist. Ein Ausfall Kritischer Infrastruktur birgt das unmittelbare Risiko des Zusammenbruchs der Grundversorgung für einzelne Personen oder ganze Teile der Bevölkerung.

Gemäß BSI-Gesetz § 2 Abs 10 sind Kritische Infrastrukturen jene, deren Ausfall oder Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit verursachen kann.

Diese Begriffsbestimmung leitet sich aus der EU Richtlinie 2008/114 ab, welche die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen und die Gesundheit, Sicherheit und das wirtschaftliche oder soziale Wohlergehen der Bevölkerung als Aufgabe Kritischer Infrastruktur begreift.

Aus diesem Grund ergibt sich die Notwendigkeit des besonderen Schutzes Kritischer Infrastrukturen und die Bereithaltung von Notfallplänen, -reserven und -personal. Der Ausfall Kritischer Infrastruktur ist nicht tolerierbar.

Um dieser Anforderung mit endlichen Ressourcen gerecht zu werden, müssen Risiken bestimmt und Maßnahmen zur Reduktion der Risiken auf ein akzeptables Maß geplant, umgesetzt, geprüft, kontinuierlich aufrechterhalten und verbessert werden. Kritische Infrastrukturen beinhalten immer physische Komponenten. Durch die Digitalisierung von Kommunikation und Steuerung ist Software bzw. programmierbare Logik aber ein unverzichtbarer Bestandteil Kritischer Infrastrukturen geworden. Diese können daher auch als *Cyber-physische Systeme* bezeichnet werden. Das bedeutet auch, dass es nicht mehr genügt, nur die physische Sicherheit und den Schutz von Anlagen zu betrachten. Schutz- und Sicherheitsmaßnahmen beinhalten immer auch IT—Sicherheit.

Dabei fällt in der Praxis auf, dass der Begriff "*Sicherheit*" bzw. "*öffentliche Sicherheit*" oft nur einseitig verstanden wird. Denn im deutschen Sprachgebrauch werden sehr verschiedene Themenbereiche unter dem Begriff "Sicherheit" versammelt. Wenn wir Begriffe wie *Schutz*, *Sicherheit* oder auch *IT—Sicherheit* verwenden, kann ein gemeinsames Verständnis also nicht vorausgesetzt werden. Klare Begrifflichkeiten sind aber

Dieser Artikel ist zuerst Blog der AG KRITIS erschienen. (Siehe https://ag.kritis.info/2020/04/03/)

alleine schon deshalb wichtig, weil die unterschiedlichen Bereiche deutlich unterschiedliche und oft auch widersprüchliche Anforderungen und Ziele haben.

In der deutschen Ausgabe der EU Richtlinie 2008/114 findet sich zur Definition Kritischer Infastrukturen nur der mehrdeutige Begriff "*Sicherheit*", obwohl die englische Ausgabe derselben EU Richtlinie nach "*Safety*" und "*Security*" differenziert:

> "*kritische Infrastruktur* bezeichnet die in einem Mitgliedstaat gelegene Anlage, ein System oder ein Teil davon, die von wesentlicher Bedeutung für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen, der Gesundheit, der Sicherheit und des wirtschaftlichen oder sozialen Wohlergehens der Bevölkerung sind und deren Störung oder Zerstörung erhebliche Auswirkungen auf einen Mitgliedstaat hätte, da diese Funktionen nicht aufrechterhalten werden könnten"
> 2008/114/EU

Es ist also sinnvoll die Bereiche *Safety* und *Security* genauer zu differenzieren, auch wenn dieser Unterschied im deutschen Sprachgebrauch nicht offensichtlich ist.

2 Konflikte von Safety und Security

Wo der Brandschutz einen lebensrettenden Notausgang sieht (*Safety*), sieht der Sicherheitsberater eine Schwachstelle im Zugangsschutz (*Security*). Dieses simple Beispiel zeigt den Konflikt, der oft zwischen dem besteht, was im Englischen als *Security* und *Safety* unterschieden wird. Im Kern des Konflikts steht die Frage, welche Sicherheit für welche Schutzfunktionen benötigt werden und welche Schutzmaßnahmen notwendige Sicherheitsmaßnahmen untergraben. Die Beschäftigung mit dieser Frage ist notwendig, weil die beiden Seiten oftmals von unterschiedlichen Experten bearbeitet werden. Kommunikation ist notwendig, um die unterschiedlichen Ziele miteinander zu verbinden und Missverständnisse zu vermeiden.

Kommunikation setzt ein gemeinsames Verständnis der Begrifflichkeiten voraus, weshalb wir im Folgenden den Versuch einer Begriffsbestimmung der *Sicherheit* durch die zwei Begriffe *Safety* und *Security* unternehmen wollen. In der Literatur finden sich verschiedene Merkmale die zur Unterscheidung herangezogen werden.

1. Unterscheidung nach Schadensursache:
   - *Safety* als Schutz eines Systems vor zufälligen, nicht-bewusst herbeigeführten Schadereignissen, z.B. Wetterphänomene oder Fehlbedienung.
   - *Security* als Schutz eines Systems vor bewußt herbeigeführten, zielgerichteten Schadereignissen, z.B. Cyberangriffe.
2. Unterscheidung nach Art des Schadens und nach Schädigungsrichtung:
   - *Safety* als Schutz vor Personenschäden, in der Regel durch das betrachtete System.
   - *Security* als Schutz vor allen Schadensarten am betrachteten System.

Diese Situation zeigt dass auch grundlegende Begriffe komplexer sind als vielfach angenommen. Das ist natürlich unbefriedigend und erfordert, dass das Verständnis der Sicherheitsgrundbegriffe neu ausgehandelt werden muss.

3 *Safety* und *Security* nach dem Ursachekriterium

Von *Safety* sprechen wir, wenn es darum geht Anlagen, Prozesse oder Personen vor Beeinträchtigung durch ungesteuerte, zufällige oder natürliche Ereignisse zu schützen. In diese Klasse fallen Ereignisse die durch "ungewollte Fehlbedienung" ausgelöst werden, ebenso wie die Beschädigung durch Umweltereignisse wie Erdbeben oder Stürme.

Demgegenüber verstehen wir *Security* als Verhinderung oder Vermeidung von unerlaubter, absichtlicher Beeinflussung, mit dem Willen zur Schädigung von *Werten* (*Assets*). Im Gegensatz zur Safety sind der wesentliche Faktor im Bereich Security die *Angreifer* (*Attacker* oder auch *Threat Agents*), die sich insbesondere dadurch auszeichnen, dass sich ihre Fähigkeiten und ihr Verhalten schlecht vorhersagen lassen. Während es vergleichsweise einfach ist, die erwarteten Sturmereignisse in einer Region historisch aufzuzeichnen, statistisch zu beschreiben und damit zu prognostizieren, ist das Verhalten von Angreifern nicht durch empirische Beobachtung vorhersagbar. Schlimmer noch, es ist anzunehmen, dass, wenn Sicherheitsmaßnahmen auf bekannte Angriffsmuster optimiert werden, sich die Angreifer anpassen und insbesondere die verbleibenden Lücken oder genau die Sicherheitsmaßnahmen selbst angreifen.

Die Definition über die Schadensursache ist für die Planung von Schutzmaßnahmen einfach anzuwenden. Bei der Analyse und Reaktion auf Schadensereignisse ist jedoch gerade dieses einfache Kriterium der bewussten Schädigung schwer zu ermitteln. Denn es erfordert eine Attribution der Schadensursache bzw. der Verursacher. Eine eindeutige Attribution ist in einer digitalen Welt aber im Allgemeinen nicht möglich. Deshalb ist es sinnvoll, zusätzlich die Definition nach anderen Kritierien zu berücksichtigen.

4 *Safety* und *Security* nach dem Schadenskriterium

Das Kriterium der Schadensrichtung besagt, dass die Unterscheidung sich dadurch ergibt, ob ein möglicher oder tatsächlicher Schaden am betrachteten System oder ein Schaden durch das betrachtete System an einer anderen Sache vorliegt. Der Begriff *Safety* bezieht sich deshalb auf Schaden, der durch das System selbst entsteht, z.B. ein Zug dessen Bremssystem versagt. Der Begriff *Security* bezieht sich auf Schadenswirkung am System.

Das informelle Glossar der Internet Enginieering Task Force, welche wesentliche Internet Standards spezifiziert hat, empfiehlt die folgende Definition:

> **Safety**: "The property of a system being free from risk of causing harm (especially physical harm) to its system entities." RFC 4949

Sicher, im Sinne von *Safety*, ist ein System dann, wenn kein Risiko besteht, dass von einem betrachteten System Schaden ausgeht.

Für den Begriff *Security* werden, je nach Kontext drei unterschiedliche Definitionen angeboten. Als Zustand wird *Security* als Ergebnis der Einführung und Aufrechterhaltung von Maßnahmen zum Schutz des Systems verstanden. *Security* kann weiterhin als Oberbegriff für genau diese Maßnahmen verstanden werden. Als Gegenstück zur *Safety* wird *Security* analog zur IT-Sicherheit als Zustand in dem ein System frei ist von möglichem Schaden von aussen, in Bezug auf die Unmöglichkeit von unauthorisiertem Zugang, Veränderung, oder Datenverlust, aber auch zufälligen Schadenseinwirkungen.

> **Security**: "A system condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss." RFC 4949

Safety und *Security* unterscheiden sich auch nach der Art des Schadens. *Safety* wird immer als ein Schutz vor Personenschäden verstanden, also Verletzung oder Tod von Menschen.

Demgegenüber bezieht sich *Security* sowohl auf den Schutz vor Personenschäden wie auch vor materiellen und ideellen Schäden. Deshalb ist es sinnvoll, bei *Security* zusätzlich nach *IT Security* und *Physical Security* zu unterscheiden, um besser nach Schadensart differenzieren zu können.

Der Begriff *IT-Sicherheit* bzw. *IT Security* oder *Computer Security* im Englischen kann als Spezialfall der oben definierten *Security* betrachtet werden. Informationstechnik (IT) ist ein wesentliches Element der aktuellen Veränderungen in Kritischen Infrastrukturen. IT-Sicherheit geht üblicherweise von der Definition des National Institutes for Standards and Technology (NIST) aus. Das NIST definiert *Computer Security* als die Sicherstellung von Integrität, Geheimhaltung und Verfügbarkeit von Systemen und Daten:

> **Computer Security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the *integrity*, *availability*, and *confidentiality* of information system resources (includes hardware, software, firmware, information/data, and telecommunications). NIST SP 800-12

Der Begriff *Physical Security* kommt aus dem Militär und bezeichnet im engeren Sinne alle physischen Schutzmaßnahmen gegen unerlaubten Zugriff. Ein vergleichbarer deutscher Begriff ist Objektschutz. Im weiteren Sinne umfasst *Physical Security* alle Schutzmaßnahmen durch Sicherheitskräfte, auch im nichtmilitärischen Bereich wie zum Beispiel durch die Polizei.

Während die *IT Security* sich überwiegend auf finanzielle *Werte* bzw. Schäden konzentriert, ist die *Physical Security* mit finanziellen (Raub), menschlichen (Mord, Verletzung, Entführung, Stalking), ideellen (Rufschädigung, Beleidigung), wirtschaftlichen (Sabotage) und gesellschaftlichen (Terrorismus) Schäden bzw. *Werten* befasst.

5 *Safety* und *Security* in Cyber-physischen Systemen

Allgemein werden Systeme die aus verknüpften physischen und digitalen Prozessen bestehen als *Cyber-physisches System* bezeichnet. In Cyber-physischen Systemen lässt sich die Beschränkung auf *IT Security* nicht mehr aufrechterhalten, weil hier grundlegende Eigenschaften von IT-Prozessen und -Artefakten nicht gelten. Zum Beispiel sind physische Assets, anders als Daten, nicht beliebig, nahezu kostenfrei und instantan kopierbar. Auf der anderen Seite sind IT-Prozesse meist formal und rigide (eben *digital*), während physische Prozesse regelmäßig Spielräume sowohl bei den Ergebnissen, als auch bei den (menschlichen) Entscheidungen benötigen.

Die *Security* Cyber-physischer Systeme muss im Vergleich mit *IT Security* deutlich mehr Schadensarten berücksichtigen, da alle Werte gemäss den oben aufgeführten Definitionen Kritischer Infrastruktur zu schützen sind. Insbesondere handelt es sich bei Kritischer Infrastruktur um Anlagen und Systeme, die immer auch menschliche Schäden bewirken können (*Safety* Schadensart) und daher sowohl gegen *Safety* wie *Security* Ereignisse (Ursachen) zu schützen sind.

Dabei können Konflikte zwischen *Safety* und *Security* Schutzmaßnahmen kaum vermieden werden. *Safety* Maßnahmen wie Redundanz oder Notfall-Kontrollsysteme können gerade erst Angriffe ermögli-

chen. Und *IT Security* Maßnahmen können potentiell Safety Maßnahmen blockieren.

Während in physischen Prozessen schon durch räumliche Nähe eine grundsätzliche, und flexible Form von Authorisierungsprüfung besteht, sind diese in der digitalen Welt immer formal streng umgesetzt und absolut. Dies führt zum Beispiel dazu, dass der Übergang in einen - wie auch immer gearteten - Notzustand digital schwieriger Umzusetzen ist. Wir wollen das nachfolgend kurz an Beispielen demonstrieren.

Der Zugriff auf Notbremsen ist üblicherweise nicht eingeschränkt. Jede Person, welche sich in räumlicher Nähe befindet (sowie eine minimale Körpergröße und physische Kraft mitbringt) soll eine Notbremsung auslösen können. Eine Authorisierungsprüfung findet nicht statt. Der Vorgang der Notbremsung stellt dazu mit einer hohen Wahrscheinlichkeit sicher, dass die auslösende Person für diese Aktion verantwortlich gemacht werden kann. Bei Notbremsen findet eine Abwägung statt, welche das Missbrauchspotential durch unauthorisierte Auslösung einer Bremsung (Security) gegen den möglichen Schaden eines Feuers oder einer vermeidbaren Kollision (Safety) abwägt. Darüber hinaus ist die Motivation der denkbaren Angreifer für einen Missbrauch sehr gering. In Kombination mit der möglichen Strafhöhe, ist der Missbrauch anscheinend sehr selten.

Eine andere Art der Abwägung findet bei Notrufnummern statt. Obwohl die Missbrauchsrate (Security) der Polizei- und Feuerwehr-Notruftelefonnummern signifikant ist, überwiegt der Nutzen in prozentual wenigen Fällen großen Schaden (Safety) verhindern zu können.

6 Fazit

Schon bei diesen einfachen Beispielen zeigt sich, dass die Anforderungen von *Safety* und *Security* nicht einfach in Einklang zu bringen sind und sich Maßnahmen oftmals wechselseitig beeinflussen. Es ist offensichtlich, das insbesondere Schutzmaßnahmen (im Sinne der Safety) gegen Angriffe auf die Verfügbarkeit und Integrität geschützt werden müssen (im Sinne der Security). Schutzsysteme sind regelmäßig selbst "kritisch" für den Schutz vor Schaden an Leib und Leben oder für den Erhalt kritischer Funktionen. Eine Beeinflussung der Schutzsysteme durch Angreifer ist ein wesentliches Ziel für den Betrieb solcher Anlagen. In diesem Sinne gibt es keine *Safety* ohne *Security*.

Security ist wiederum auch kein Selbstzweck. Die primäre Aufgabe kritischer Systeme ist die Versorgung der Gesellschaft mit absolut notwendigen Diensten und Gütern. Das bedeutet aber auf der anderen Seite nicht, dass wir im Namen der Notfallvorsorge auf grundsätzliche Prinzipien und Regeln unserer Gesellschaft verzichten können. Gerade in der Krise und ihrer Bewältigung zeigt sich oftmals das wahre Gesicht eines Menschen — und vielleicht auch einer Gesellschaft.

In diesem Wechselspiel der Anforderungen gibt es sicher viele offene Fragen und wenige endgültige Antworten. Dieser Text ist deshalb auch eher als Anfang einer Diskussion zu verstehen, denn als allumfassende Lösung.

7 Quellen

Grundlage des vorgestellten Papieres war eine gründliche Recherche in Standards und Lehrbüchern in den Bereichen *Safety* und *Security*, mit einem Schwerpunk, aber nicht beschränkt auf, industrielle Anwendungen und Kritische Infrastruktur. Zum Erstaunen der Autoren konnten wir keine kanonische Definition und Differenzierung der beiden Begriffe in der einschlägigen Literatur finden. Im Artikel finden sich nur Quellen, in denen wir nutzbare Definitionen auffinden konnten. Wesentlich ist aber auch welche Quellen zu der Einschätzung geführt haben, dass eine grundlegende Definition der Begriffe notwendig ist. In diesem Abschnitt werden insbesondere die verwandten Quellen behandelt die nicht zur Definition von *Safety* und *Security* beigetragen haben.

Dieser Abschnitt gibt einen Überblick über die aufgefundenen Quellen, welche für diesen Artikel aufgefunden und herangezogen wurden.

Die bekannteren Lehrbücher aus der IT-Sicherheit thematisieren den Konflikt zwischen *Safety* und *Security* nicht umfassend. (Eckert, 2018; Bishop, 1992; Stallings und Brown, 2015) Bemerkenswert ist darüber hinaus, dass selbst Lehrbücher zur *Security* von Industriesystemen, einer Domäne in der Schutzeinrichtungen gegen Naturereignisse, Fehlbedienungen oder Schwankungen in Materialien fest integriert sind, keine Differenzierung dieser grundlegenden Begriffe umfassen. (Knapp und Langill, 2014; Colbert und Kott, 2016)

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) liefert mit den BSI-Standards *BSI 100* und der Fortschreibung als *BSI 200* wesentliche Grundlagen im Bereich IT-Sicherheit. Ebenso wie die verwandten internationalen Standards ISO/IEC 27001; ISO 31000, wird *Safety* nicht thematisiert. In der aktuellen Version des ersten Teils BSI 200-1 wird der Begriff IT-Sicherheit von Informationssicherheit und Cyber-Sicherheit unterschieden. Damit findet eine deutliche Erweiterung der bisher kanonischen CIA-Triade aus NIST SP 800-12 statt. Letztere Definition von *IT-Security* als Vereinigung der hinreichenden Sicherheitsziele *Confidentiality*, *Integrity*, und *Availability* gilt bis heute als gemeinsamer Definitionskern der IT-Sicherheit.

Der Standard IEC 62351 *Data and communication security* greift im Glossar IEC 62351-2 zur Definition von *Security* auf mehrere Quellen zurück. Die Definitionen beschreiben *Security* entweder als Zustand der Unverletzlichkeit gegenüber Angriffen oder als Aspekte in Bezug auf die Erreichung einer Liste von Sicherheitseigenschaften. Dies entspricht einer Form des Verursacherkriteriums.

In den *Common Criteria for Information Technology Security Evaluation* CC V3.1 R5 ist *Security* verstanden als in Bezug auf den Schutz von Werten.

Allen obigen Quellen ist gemein, dass sie sich ausschließlich auf den Begriff *Security* beziehen. Die Beschreibungen Grenzen sich nicht vom Begriff *Safety* ab, was nur dann sinnvoll scheint, wenn es praktisch keine Berührungspunkte gibt. Die Beispiele in unserem Text zeigen allerdings auf, dass es nicht möglich ist das eine ohne das andere zu betrachten.

Im, in der deutschen Industrie weithin genutzten, Bundesverbandder Energie-undWasserwirtschaft e.V. (BDEW) Whitepaper "Anforderungen an sichere Steuerungs- und Telekommunikationssysteme" wird lediglich der Begriff *Safety* im Glossar als "Freiheit von untragbaren Risiken" definiert. Selhofer, Tidten und Beirer, 2018 Eine Erklärung des Attributs *sicher* oder von *Sicherheit* findet nicht statt und sind nur indirekt über die Spezifikation von *Sicherheitsanforderungen* beschrieben.

Das *Aeronautical Information System Security Glossary* (ER-013) bezieht sich auf die *Aeronautical Information System Security (AISS) Framework Guidance* von 2015 in welcher der Zweck von *Security* als Sicherstellung von *Safety* beschrieben wird, allerdings nur bezogen auf die Luftfahrt.

Einzige aufgefundene Quelle im deutschen Bereich in der *Safety* und *Security* explizit abgegrenzt werden ist *Safety vs. Security: Der Unterschied einfach erklärt*. Dabei handelt es sich aber lediglich um die Festlegung eines einzelnen Autoren, ist aber vergleichbar mit der Definition im informellen *Internet Security Glossary, Version 2* der Internet Engineering Task Force (IETF).Diese Quelle ist die einzige aufgefundene Quelle, in der beide Begriffe trennscharf definiert werden. Darüber hinaus werden zwei übliche Definitionsarten des Begriffs *Security* angeboten:

> "safety (I) The property of a system being free from risk of causing harm (especially physical harm) to its system entities. (Compare: security.) [...] security
> 1a. (I) A system condition that results from the establishment and maintenance of measures to protect the system.
> 1b. (I) A system condition in which system resources are free from unauthorized access and from unauthorized or accidental change, destruction, or loss. (Compare: safety.)" (RFC 4949)

Auch wenn die Konflikte zwischen *Safety* und *Security* nicht aus der fehlenden Differenzierung in den Quellen und der begrifflichen Zusammenfassung zu *Sicherheit* in vielen Sprachen begründet sind, wird die Situation dadurch nicht verbessert.

Referenzen

Bishop, Matt (1992). *Introduction to computer security*. Bd. 11. 2, S. 121–127. ISBN: 0321247442. DOI: 10.1016/0167-4048(92)90036-Q. arXiv: arXiv:1011.1669v3. URL: http://link.springer.com/10.1007/978-1-4471-6663-4.

Bundesamt für Sicherheit in der Informationstechnik (2017). *BSI-Standard 200-1: Managementsysteme für Informationssicherheit*. URL: https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard201/ITGStandard201_node.html.

Colbert, Edward JM und Alexander Kott (2016). *Cybersecurity of SCADA and other Industrial Control Systems*. Bd. 66. Springer.

CC V3.1 R5 (2017). *Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components*. Techn. Ber. Revision 5. Version 3.1. URL: https://www.commoncriteriaportal.org/cc/.

2008/114/EU (23. Dez. 2008). *Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*. OJ L 345, p. 75–82. URL: https://eur-lex.europa.eu/eli/dir/2008/114/oj.

2013/40/EU (12. Aug. 2013). *Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA*. OJ L 218, p. 8–14. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj.

Eckert, Claudia (2018). *IT-Sicherheit. Konzepte-Verfahren-Protokolle (10., erweiterte und aktualisierte Auflage)*. 10. Aufl. Berlin, Boston: Walter de Gruyter.

ER-013 (2015). *ER-013 - Aeronautical Information System Security Glossary*. Techn. Ber. The European Organisation for Civil Aviation Equipment. URL: https://eshop.eurocae.net/eurocae-documents-and-reports/er-013.

Geiger, Markus. *Safety vs. Security: Der Unterschied einfach erklärt*. URL: https://www.sichere-industrie.de/safety-security-unterschied-erklaert-kombination-ziele-industrial-security/.

Guttman, Barbara und E. Roback (1995). *An Introduction to Computer Security: the NIST Handbook*. NIST SP 800-12. NIST. DOI: 10.6028/nist.sp.800-12. URL: https://doi.org/10.6028/NIST.SP.800-12.

IEC 62351-2 (2007). *IEC 62351-2 Ed.1: Data and Communication Security - Part 2: Glossary of terms*.

ISO/IEC 27019 (Okt. 2017). *Information technology — Security techniques — Information security controls for the energy utility industry*. Standard ISO/IEC 27019-2017. Version 2017-10. ISO/IEC.

ISO 31000 (2018). *ISO 31000:2018 Risk management — Guidelines*. Standard. Version 2. ISO/TC 262

Risk management. URL: https://www.iso.org/standard/65694.html.

ISO/IEC 27001 (2019). *ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements*.

Knapp, Eric D und Joel Thomas Langill (2014). *Industrial Network Security: Securing critical infrastructure networks for smart grid, SCADA, and other Industrial Control Systems*. Syngress.

Selhofer, Armin, Kay Tidten und Stephan Beirer (24. Mai 2018). *Whitepaper Anforderungen an sichere Steuerungs- und Telekommunikationssysteme*. Oesterreichs E-Wirtschaft und BDEW Bundesverband der Energie- und Wasserwirtschaft e.V. URL: https://www.bdew.de/media/documents/Awh_20180507_OE-BDEW-Whitepaper-Secure-Systems.pdf.

Shirey, R. (Aug. 2007). *Internet Security Glossary, Version 2*. Techn. Ber. IETF. URL: https://tools.ietf.org/html/rfc4949.

Stallings, William und Lawrie Brown (2015). *Computer Security: Principles and Practice*. Third. Pearson Educated Limited, S. 840. ISBN: 978-1-292-06617-2.