acatech DISKUSSION

Beiträge zu einer Systemtheorie Sicherheit

Jürgen Beyerer, Petra Winzer (Hrsg.)

acatech
DEUTSCHE AKADEMIE DER TECHNIKWISSENSCHAFTEN

Inhalt

1 Problemstellung und Zielsetzung einer „Systemtheorie Sicherheit“

Prof. Dr.-Ing. habil. Jürgen Beyerer
Fraunhofer-Institut für Optronik, Systemtechnik und Bildauswertung IOSB
Lehrstuhl für Interaktive Echtzeitsysteme
am Institut für Anthropomatik und Robotik
Karlsruher Institut für Technologie KIT

Sicherheit ist ein fundamentales menschliches Grundbedürfnis, das in der Maslow'schen Bedürfnispyramide direkt auf die physiologischen Bedürfnisse folgt.[1] Sicherheit ist aber auch ein Grundbedürfnis für Unternehmen, Organisationen und unseren Staat.

Dabei ist der deutsche Begriff Sicherheit ziemlich vielschichtig. Er bezieht sich sowohl auf Gefahren durch natürliche Phänomene als auch durch andere Menschen und vom Menschen geschaffene Artefakte und Systeme. Solange es um Sicherheit geht, bei der keine absichtliche Gefährdung durch den Menschen im Spiel ist, spricht man im Englischen spezifischer als im Deutschen von *Safety*. Steckt menschliche Absicht und Intelligenz hinter einer Gefährdung, hat man in der englischen Sprache mit *Security* ebenfalls einen differenzierteren Begriff parat. Im weiteren Sinne bezieht der Begriff Sicherheit auch noch die Zuverlässigkeit (im Englischen: *Reliability*) mit ein. Um diese drei Teilaspekte der Sicherheit adäquat ausdrücken zu können, hat sich der Begriff der „Verlässlichkeit“ etabliert.[2]

Von besonderem gesellschaftlichem Interesse ist die Sicherheit soziotechnischer Systeme.[3] Soziotechnische Systeme sind komplex, und ihre Sicherheit involviert viele Disziplinen: Technik- und Naturwissenschaften, Rechts-, Geistes- und Sozialwissenschaften. Die Motivation für diese Veröffentlichung ist, dass es bislang keine durchgängige, allgemeine Theorie gibt, mit der sich Sicherheit derart komplexer Systeme behandeln lässt und die eine einheitliche, disziplinübergreifende Theorienbasis zur Verfügung stellt. Die Entwicklung einer solchen ganzheitlich angesetzten Theorie erfordert einen gründlichen Diskussionsprozess zwischen den betreffenden Disziplinen und stellt sowohl eine große Kommunikations- als auch eine Abstimmungsherausforderung dar. Die Verfasserinnen und Verfasser dieses Buchs sind der Überzeugung, dass es sich lohnt, eine solche übergreifende Theorie für die Sicherheit in Angriff zu nehmen, und haben sich entsprechend auf den Weg gemacht, erste einschlägige Beiträge zu erarbeiten.

In der Geschichte von Wissenschaft und Technik gibt es viele Beispiele für Gebiete, die erst nach Erscheinen einer grundlegenden Theorie eine rasante Entwicklung genommen haben. Ein schönes Exempel ist die Maxwell'sche Theorie des Elektromagnetismus:[4] Bis James Clerk Maxwell im Jahr 1865 die nach ihm benannten Maxwell-Gleichungen veröffentlichte, gab es eine Vielzahl noch nicht schlüssig miteinander verwobener Einzelerkenntnisse und Teiltheorien von Erfindern und Forschern wie André-Marie Ampère, Charles Augustin de Coulomb, Michael Faraday, Benjamin Franklin, Luigi Galvani, Carl Friedrich Gauß, Hans Christian Ørsted, Alessandro Volta, Wilhelm Eduard Weber und vielen anderen. Maxwell schaffte es schließlich mit seiner Theorie, alle bekannten Phänomene der klassischen Elektrodynamik mit einem kompakten Formelapparat zu beschreiben und sie damit genau zu berechnen. Der Siegeszug der Elektrotechnik wurde zweifellos besonders durch die Bereitstellung dieser grundlegenden Theorie beflügelt.

Ein weiteres Beispiel ist die Regelungstechnik und die dahinterstehende Kybernetik. Zu Beginn des 20. Jahrhunderts war die Regelungstechnik noch stark nach technologischen Ausprägungen gegliedert. Fliehkraftregler zur Drehzahleinhaltung rotierender Kraftmaschinen, Thermostate zur Temperaturregelung, elektrische Regler zur Konstanthaltung von Spannungen und Strömen und so weiter hatten überwiegend eigene Beschreibungsweisen und waren noch nicht in einer kohärenten Wissenschaft aufgegangen. Vor allem in den 40er Jahren des vergangenen Jahrhunderts wurde maßgeblich durch Norbert Wiener und Herrmann Schmidt eine vereinheitlichende Sicht auf die Regelungstechnik entwickelt.[5] Wiener begründete die übergeordnete Lehre der Kybernetik, welche die grundlegenden Gemeinsamkeiten von

1 | Vgl. Maslow 1943.
2 | Vgl. Bertsche et al. 2018.
3 | Unter einem soziotechnischen System versteht man eine organisierte Menge von Menschen und mit diesen verknüpfte Technologien, welche in einer bestimmten Weise strukturiert sind, um ein spezifisches Ergebnis zu produzieren; vgl. Wikipedia 2018.
4 | Vgl. Maxwell 1865.
5 | Vgl. Fasol et al. 2006.

Regelungsvorgängen in Natur und Technik beschreibt, abstrahiert und erklärt.[6] Auf Basis dieser fundamentalen theoretischen Grundlage entwickelte sich dann in der Folgezeit die Regelungstechnik zu einer sehr reichen wissenschaftlichen und technischen Disziplin.

Wie bereits zu Beginn erwähnt, gibt es für die Sicherheit soziotechnischer Systeme bis heute keine Theorie, die alle oben genannten Disziplinen umfasst und eine technologie- und anwendungsdomänenübergreifende Methodik zur Verfügung stellt, mit der eine umfassende formale Problembeschreibung gelingt und komplexe Sicherheitssysteme im soziotechnischen Kontext untersucht, entworfen und verbessert werden können. Die Sicherheitsaspekte Safety, Security und Zuverlässigkeit werden in der Regel unnötigerweise separat betrachtet, sodass mögliche Synergiepotenziale eines ganzheitlichen Ansatzes ungenutzt bleiben.

Um diese methodischen Defizite zu beseitigen, bedarf es einer mathematisch fundierten **Systemtheorie für die Sicherheit**, die von den Spezialitäten der Disziplinen und Technologien abstrahiert, gleichzeitig aber ausdrucksstark genug ist, um die Erfordernisse der involvierten Disziplinen ausreichend abzudecken. Eine solche Theorie muss bemüht sein, über die Disziplinen hinweg einheitliche Begriffe zu definieren und ein gemeinsames Verständnis zu schaffen. Außerdem muss sie auf einem geeigneten Abstraktionsniveau die grundlegenden Wirkungsmechanismen, die in Bezug auf Sicherheit in allen Systemen Geltung besitzen, herausarbeiten. Allerdings ist eine formale Deskription aller sicherheitsrelevanten Eigenschaften, Belange und Mechanismen nur ein erster unverzichtbarer Schritt. Um zielgerichtet und konstruktiv die Sicherheit soziotechnischer Systeme zu analysieren, zu planen, zu verbessern und schließlich zu optimieren, bedarf es auch geeigneter Maße und Metriken, um Sicherheit zu bewerten. Und es braucht einen Kalkül, der über die reine Beschreibung hinaus auch Schlussfolgerungen erlaubt, mit dem man also „rechnen" kann. Bei alledem muss aber auch auf der Beherrschung der Komplexität von aus einer Systemtheorie Sicherheit resultierenden Modellen und Algorithmen, die sich unter anderem aus der Komplexität realer soziotechnischer Systeme ergibt, ein besonderes Augenmerk liegen.

Eine Systemtheorie Sicherheit kann und muss selbstverständlich auf wohl etablierte Gebiete aufsetzen und sollte sich daraus wie aus einem Baukasten bedienen, wie zum Beispiel aus der Informatik, der Systemtheorie, der Spieltheorie, der statistischen Entscheidungstheorie, dem Systems Engineering und der Kybernetik.

Die Förderung der Sicherheitsforschung der letzten Jahre sowohl in Deutschland als auch durch die Europäische Union hat viele sehr gute Ergebnisse hervorgebracht. Sie war aber überwiegend szenario- und anwendungsgetrieben, setzte also gewissermaßen auf eine Bottom-up-Herangehensweise, um konkrete Sicherheitsherausforderungen durch die Forschung zu traktieren. Das Streben nach einer übergreifenden Systemtheorie Sicherheit ergänzt die Sicherheitsforschung um eine wissenschaftliche Top-down-Perspektive und kann zum Synergiestifter zwischen unterschiedlichen speziellen Vorhaben in der Sicherheitsforschung werden.

Im Rahmen des Themennetzwerks Sicherheit der Deutschen Akademie der Technikwissenschaften acatech wurde in den letzten drei Jahren intensiv mit dieser übergeordneten Fragestellung einer Systemtheorie für die Sicherheit gerungen. In einer losen Folge von Workshops wurden von einer interdisziplinär zusammengesetzten Gruppe von Wissenschaftlerinnen und Wissenschaftlern erste Beiträge zu einer generalisierenden Systemtheorie für die Sicherheit in einer konstruktiv kritischen Atmosphäre offenen wissenschaftlichen Dialogs entwickelt. Der vorliegende Band stellt diese frühen Ergebnisse nun der Fachgemeinde der Sicherheitsforschung und der interessierten Öffentlichkeit zur Diskussion.

Im Beitrag von Schlüter und Winzer wird die Rolle des Systems Engineering für die Bereitstellung eines disziplinübergreifenden Denkmodells und eines Vorgehenskonzepts herausgearbeitet.[7] Mit ihrem Generic-Systems-Engineering-Ansatz (GSE-Ansatz) stellen sie allgemein ein mögliches Fundament vor, auf das sich eine Systemtheorie Sicherheit abstützen könnte. An einem konkreten Beispiel werden die Vorteile von GSE dargelegt.

Der Beitrag von Schnieder und Schnieder widmet sich zwei grundlegenden Problemstellungen einer Systemtheorie Sicherheit.[8] Für eine durchgängige, eindeutige Begriffsbildung wird auf Basis der Linguistik ein neues formales Begriffskonzept eingeführt: mittels Klassendiagrammen der Unified Modeling Language (UML). Außerdem werden verschiedene kybernetische Ansätze, probabilistische Modelle und Petrinetze zur Formalisierung von dynamischen Prozessen vorgestellt, mit denen die logische, unsicherheitsbehaftete, temporale Entwicklung sicherheitsrelevanter Abläufe modelliert werden kann.

Im Abschnitt von Bertsche et al. wird der Sicherheitsbegriff weiter gefasst, indem über die Aspekte *Safety* und *Security* hinaus die Zuverlässigkeit von Komponenten, Teilsystemen und

6 | Vgl. Wiener 1948.
7 | Vgl. Schlüter/Winzer 2018.
8 | Vgl. Schnieder/Schnieder 2018.

Systemen miteinbezogen wird.[9] Das führt zum Begriff Verlässlichkeit, der aus Sicht einer sicherheitsbedürftigen Instanz, die hinsichtlich ihrer Gefährdung alle möglichen Ursachen der Beeinträchtigung ihrer Sicherheit gleichermaßen berücksichtigen möchte, eine ganzheitliche Konzeption darstellt.

Die deutsche Begriffsbildung bezüglich Verlässlichkeit geht auf den von J. Laprie geprägten Begriff der Dependability zurück.[10] Als wichtige wegbereitende Arbeiten zur Etablierung des Begriffs Verlässlichkeit in den Technikwissenschaften sind hier auch die weiter zurückliegenden Veröffentlichungen aus der Forschungsgruppe von Eckehard Schnieder[11] zu nennen.

Der Aufsatz von Beyerer und Geisler versucht mit Mitteln der statistischen Entscheidungstheorie und einer Bayes'schen Interpretation von Wahrscheinlichkeit als Grad des Dafürhaltens (Degree of Belief), eine vereinheitlichende Formalisierung Safety- und Security-bezogener Risiken zu schaffen.[12] Mit der Definition eines Rollenkonzepts (Schutzbedürftiger, Gefährder, Schützer) sowie dem Konzept von differenzierten Flanken der Verwundbarkeit wird zusammen mit einer zeitlichen Dynamisierung und einer örtlichen Diskretisierung über Graphen eine methodische Basis vorgeschlagen, mit der soziotechnische Systeme mittels Softwareagenten simuliert werden können.

Müller-Quade beleuchtet in seinem Beitrag die Sicht der Kryptographie auf eine Systemtheorie Sicherheit.[13] Aus dieser Warte spielen vor allem Gefährdungen durch intelligente Angreifer eine Rolle, für die eine probabilistische Modellierung ungeeignet erscheint.

Der Beitrag von Vieweg bringt eine erste juristische Perspektive in die Betrachtungen ein.[14] Neben der Klärung von Begriffen werden einige Risikoszenarien dargestellt und diskutiert. Das Zusammenwirken von Rechtssetzern, Verantwortungsträgern und Entscheidern sowie Behörden und Gerichten in Bezug auf die Sicherheit soziotechnischer Systeme wird als Prozess in einem Regelkreismodell beschrieben und erklärt.

In dem Aufsatz von Raabe wird eine zweite juristische Perspektive auf das Thema Systemtheorie Sicherheit eingenommen.[15] Dabei geht es unter anderem um Risiken für den Datenschutz und die Zusammenhänge mit dem IT-Sicherheitsrecht. Insbesondere wird untersucht, inwieweit abstrakte entscheidungstheoretische Ansätze zur Modellierung solcher Risiken geeignet sind.[16]

In den folgenden Kapiteln geht es dann um spezifische Anwendungen von Ansätzen der Systemtheorie Sicherheit auf konkrete Probleme. Dabei bleibt aber trotz des ausgeprägten Anwendungsbezugs der übergreifende Anspruch der vorliegenden Veröffentlichung im Fokus. Die Beiträge von Lichte und Wolf[17] sowie von Deutschmann und Milbredt[18] befassen sich mit der Sicherheit von Flughäfen. Bei Lichte und Wolf steht die Quantifizierung der Verwundbarkeit (Vulnerabilität) dieser kritischen Infrastrukturen im Vordergrund, wobei Angriffspfade hinsichtlich einer probabilistischen Bewertung der zeitlichen Entfaltung von Gefahren hinsichtlich ihres Risikos beurteilt werden. Eine Perspektive bezüglich der Bewertung der Leistungsfähigkeit von Sicherheitsmaßnahmen auf Basis geeigneter Key-Performance-Indikatoren nimmt der Aufsatz von Deutschmann und Milbredt ein.

Im Beitrag von Labudde wird ein systemtheoretischer Ansatz zur Ausbreitung krimineller Gefahren vorgestellt.[19] Urbane Strukturen werden als Graphen modelliert, auf denen dann ein Wechselwirkungsmodell zwischen Akteuren rechnerisch durchgespielt werden kann. Akteure werden als mobile Softwareagenten modelliert, die sich auf dem Graphen aufhalten und bewegen. Auf dieser Basis können räumliche/zeitliche Simulationen durchgeführt werden, mit denen die Ausbreitung von Kriminalität untersucht und ein Predictive Policing ermöglicht werden kann.

Der Aufsatz von Gleirscher betrachtet die Gefahrenerkennung und -behandlung in autonomen Maschinen.[20] Er stellt eine werkzeugbasierte Vorgehensweise zur Modellierung von Gefahrensituationen und zur Plausibilitäts- und Vollständigkeitsbewertung entsprechender Modelle am Beispiel des automatisierten Fahrens vor.

9 | Vgl. Bertsche et al. 2018.
10 | Vgl. Laprie 1992.
11 | Vgl. Schnieder 2003, Slovak et al. 2005, Schnieder/Slovak 2007 und Müller 2015.
12 | Vgl. Beyerer/Geisler 2018.
13 | Vgl. Müller-Quade 2018.
14 | Vgl. Vieweg 2018.
15 | Vgl. Raabe 2018.
16 | Vgl. Beyerer/Geisler 2018.
17 | Vgl. Lichte/Wolf 2018.
18 | Vgl. Deutschmann/Milbredt 2018.
19 | Vgl. Labudde 2018.
20 | Vgl. Gleirscher 2018.

Im Beitrag von Weyer et al. wird ein umfassendes System für die agentenbasierte Simulation soziotechnischer Systeme vorgestellt.[21] Der Ortsbezug wird durch einen Graphen dargestellt, der eine betrachtete Liegenschaft (Infrastruktur) diskretisiert und als Aktionsfeld für die Agenten dient. Das Simulationssystem SimCo ist dabei eine zunächst semantikfreie Plattform, die erst durch eine konkrete Ausprägung von Agententypen sowie die Anpassung des Graphen an eine spezifische Liegenschaft und Aufgabe spezielle Bedeutung erhält. Hiermit lassen sich Simulationen bezüglich verschiedener soziotechnischer Systeme durchführen, um insbesondere die Beeinflussbarkeit solcher Systeme durch unterschiedliche steuernde Vorgaben zu untersuchen.

Abschließend wenden Arens und Kühne systemtheoretische Ansätze auf Fragen rund um den Schutz und die Sicherheit von Offshore-Windparks an.[22] Da es sich bei solchen Anlagen um kritische Infrastrukturen handelt, müssen Sicherheit und Risiken systematisch untersucht und bewertet werden.

21 | Vgl. Weyer et al. 2018.
22 | Vgl. Arens/Kühne 2018.