Schriften der Sudetendeutschen Akademie
der Wissenschaften und Künste
Band 34
Forschungsbeiträge
der Naturwissenschaftlichen Klasse
Seiten 27 - 134

ERNST HABIGER

Sicherheit in industriellen Bereichen

Eine Interpretation aus systemischer Sicht

Der überlegene Mensch vergisst nicht die Gefahr, wenn er in Sicherheit ist.
Konfuzius, 551 – 479 v. Chr.

Zusammenfassung

In rasantem Tempo werden im Zuge des wettbewerbsgetriebenen technischen Fortschrittgeschehens neue Technologien entwickelt, ständig weiterentwickelt und in immer komplexeren Anwendungen verbreitet. Damit erhöht sich fortlaufend das davon ausgehende Gefahrenpotential in den entsprechenden sozio-technischen Systemen, d.h. für die darin involvierten Menschen, Maschinen, Anlagen und die Umwelt. Fragen der Sicherheit spielen daher in einer zunehmend technisch geprägten Welt eine immer bedeutsamere Rolle. Ihnen wird mit technologiepezifischen Maßnahmen begegnet. Das heißt die praktizierte Sicherheitstechnik ist bislang nach anwendungsbezogenen Technikfeldern strukturiert. Hier sind systemtechnische Herangehensweisen erforderlich. Im Folgenden wird dieses weit gefächerte Problemfeld einer kurzen orientierenden Betrachtung unterworfen und ausgehend von einer elementaren Modellvorstellung einer allgemeinen Interpretation aus systemischer Sicht unterzogen.

Summary

Safety & Security in Industrial Areas
An Interpretation from a Systemic Point of View

Intense competition is driving the pace of technological progress. New technologies are being conceived, developed and integrated into evermore complex applications.This can endanger the humans, machines, assets and environments that comprise a sociotechnical system. This puts safety issues in the foreground and specific technological measures are implemented to deal with them. An approach that is more system than application oriented would be advisable. An elementary model is used to examine and interpret these diverse problems from a systemic point of view.

Einleitung

Sichtet man das sicherheitsbezogene Fachschrifttum, stößt man aus den eingangs genannten Gründen auf eine verwirrende Vielfalt von Sicherheiten und Sicherheitsinterpretationen, die sich mit unterschiedlicher Relevanz und Häufigkeit im Fachsprachgebrauch präsentieren (Tab. 1 und Tab. 2).

Dies generiert bei vielen Beteiligten, insbesondere bei Nachwuchskräften, die verständliche Frage: Ja, was ist denn eigentlich Sicherheit wirklich?

Im Folgenden wird dieses weit gefächerte Problemfeld einer kurzen orientierenden Betrachtung unterworfen und ausgehend von einer elementaren Modellvorstellung einer allgemeinen Interpretation aus systemischer Sicht unterzogen.

Themenfelder	**Auftritts-häufigkeit**	**Themenfelder**	**Auftritts-häufigkeit**
Safety	783.000.000	Web Service-Sicherheit	574.000
Security	570.000.000	Systemsicherheit	532.000
Sicherheit	66.500.000	Internetsicherheit	524.000
Aktive Sicherheit	11.700.000	Betriebssicherheit	399.000
Elektrische Sicherheit	9.410.000	Ausfallsicherheit	398.000
Passive Sicherheit	3.540.000	Gebäudesicherheit	396.000
Datensicherheit	1.850.000	Funktionssicherheit	305.000
Produktsicherheit	1.850.000	Anlagensicherheit	233.000
IT-Sicherheit	1.840.000	Maschinensicherheit	212.000
Reaktorsicherheit	1.760.000	Cyber-Sicherheit	187.000
Funktionale Sicherheit	1.510.000	Softwaresicherheit	67.900
Arbeitssicherheit	1.310.000	Gerätesicherheit	60.100
Versorgungssicherheit	1.210.000	Kommunikations-sicherheit	42.100
Informationssicherheit	1.130.000	Datenbanksicherheit	13.600
Netzwerksicherheit	828.000	Hardwaresicherheit	12.900
Computersicherheit	589.000	Kraftwerkssicherheit	6.810

Tabelle 1: Sicherheitsbezogene Themenfelder und ihre Auftrittshäufigkeit im Internet (Google-Suchergebnisse, Februar 2014)

Sicherheit aus elementarer Sicht

Nutzt man zur Beantwortung der Frage „Was ist Sicherheit“ den gesunden ingenieurmäßigen Sachverstand, kommt man unbeschadet der Tatsache, dass hierzu bereits eine Vielzahl zweckorientierter, meist unscharf formulierter Definitionen existiert (Tab. 2), sehr schnell zu dem Ergebnis, dass Sicherheitsprobleme bzw. Sicherheitsbedürfnisse technologieunabhängig grundsätzlich überall dort bestehen, wo ein in Bild 1 skizziertes elementares Bedrohungsszenario vorliegt [11]. Das heißt, dass

eine Bedrohungs- bzw. Gefahrenquelle ***Q*** vorhanden ist, von der Bedrohungen ***B*** ausgehen und mindestens eine Bedrohungssenke ***S*** existiert, d.h. ein Bedrohungsopfer bzw. ein schutzbedürftiges Objekt, das durch diese Bedrohungen einem Risiko ***R*** ausgesetzt ist, d.h. einem mit Ungewissheit belasteten Sachverhalt, der mit mehr oder weniger hoher Wahrscheinlichkeit ***W*** erwarten lässt, dass ein unerwünschtes, mit einem mehr oder weniger großen Schaden (Körperschaden, Sachschaden, Leistungsschaden, Image-Schaden) für das bedrohte Objekt einhergehendes Ereignis eintritt.

Meyers Großes Universal-Lexikon [1]: **Sicherheit** = *Zustand des Unbedrohtseins, der sich objektiv im Vorhandensein von Schutzeinrichtungen bzw. im Fehlen von Gefahr(enquellen) darstellt und subjektiv als Gewissheit von Individuen oder sozialen Gebilden über die Zuverlässigkeit von Sicherungs- und Schutzeinrichtungen empfunden wird.*
Duden [2]: **Sicherheit** = *Zustand des Sicherseins, Geschütztseins vor Gefahr oder Schaden, höchstmögliches Freisein von Gefährdungen*
The FreeDictionary [3]: **Sicherheit** = *Zustand, in dem es kein Gefahr für jemanden/etwas gibt*
Nach Bromba [4]: **Sicherheit** = 1-Risiko
VDI-Denkschrift „Technische Sicherheit“ [5]: *Unter **Technischer Sicherheit** wird begrifflich verstanden, dass ein technisches System, eine Anlage, ein Produkt über einen geplanten Zeitraum, ggfs. Über die gesamte Lebensdauer, vorgesehene Funktionen erfüllt und bei bestimmungsgemäßer Nutzung keine geschützten Rechtsgüter verletzt, d.h. weder Sachen noch Personen geschädigt werden.*
Umweltdatenbank [6]: Sicherheit = *Zustand, in dem das Risiko eines Personen- oder Sachschadens auf einen annehmbaren Wert begrenzt ist*
In Security Engineering [7]: **Sicherheit** = *Abwesenheit bekannter Angriffe auf ein System*
SIL-Handbuch [8]: **Sicherheit** = *Freiheit von unvertretbaren Risiken, die – entweder direkt oder indirekt als Ergebnis eines Sachschadens oder einer Schädigung der Umwelt - Körperverletzung oder Gesundheitsschäden hervorrufen.*
DIN VDE 31000 [9]: **Sicherheit** = *Sachlage, bei der das Risiko nicht größer als das Grenzrisiko ist*
DIN EN 61508-4 [10]: **Sicherheit** = *Freiheit von unvertretbaren Risiken*

Tabelle 2: Beispiele für Sicherheitsinterpretationen

Davon ausgehend erklärt sich für eine solche elementare Anordnung „Sicherheit“ als ein Zustand, der für ein klar abgegrenztes, bedrohtes Objekt dann besteht, wenn für dieses Objekt das Risiko im oben erklärten Sinn Schaden zu nehmen, während seiner gesamten Existenzphase einen akzeptierbaren Wert nicht überschreitet. Das grundsätzliche Ziel aller Sicherheitsbestrebungen besteht daher darin, das Wirksamwerden von Bedrohungen ***B*** weitestgehend zu unterbinden, d.h. die Eintrittswahrscheinlichkeit ***W*** eines Schaden auslösenden Ereignisses soweit wie möglich zu reduzieren. Genauer gesagt, ein ohne Schutzmaßnahmen bestehendes Risiko ***R***

mittels geeigneter technischer und organisatorischer Maßnahmen im Zuge der Systemgestaltung und des Betriebs unterhalb eines tolerierbaren Grenzrisikos R_G auf ein möglichst niedriges Restrisiko zu verbringen und dort zu halten (Abb. 1).

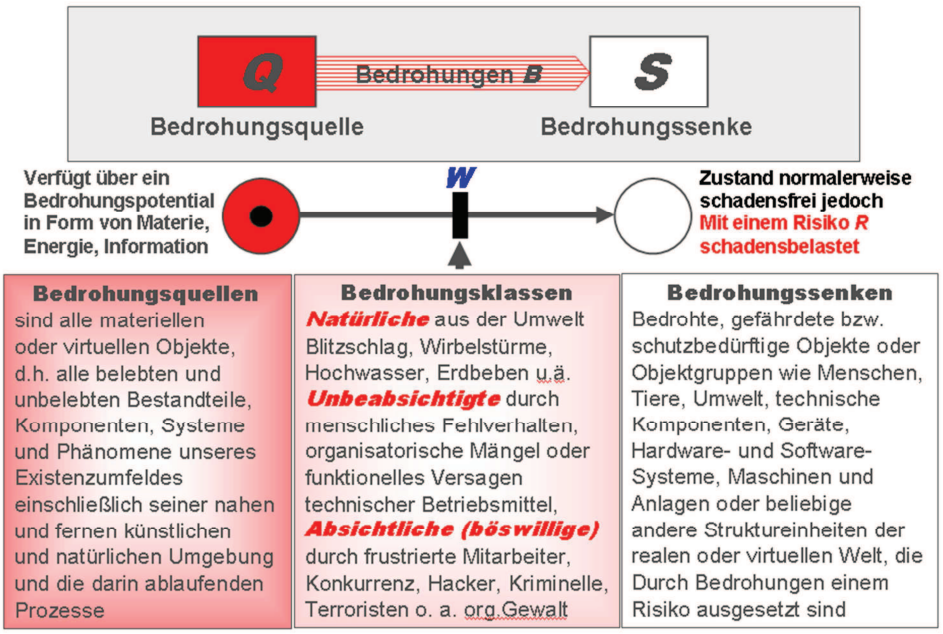

Abbildung 1: Elementares Bedrohungsszenario

E/E/PE Elektrisch/Elektronisch/Programmierbar Elektronisch

Zu diesen Maßnahmen zählen im Rahmen einer sicherheitsgerichteten Konzipierung und Ausführung technischer Systeme die gezielte Vermeidung möglicher systematischer und zufälliger Fehler, u.a. durch die Umsetzung bewährter Sicherheitsprinzipien wie Überdimensionierung, Redundanz, Hardwarediversität u.ä., durch den Einsatz sicherheitsbewährter Bauteile, Geräte, Subsysteme und Produkte, die entsprechenden Sicherheitsspezifikationen genügen sowie durch die zielgerichtete Systemausstattung mit Beobachtungs-, Überwachungs- und Sicherheitsfunktionen, um sich anbahnende, Schaden auslösende Ereignisse möglichst frühzeitig zu erkennen und durch geeignete Maßnahmen wie Alarme und automatische Gegenmaßnahmen zu unterbinden.

Ein klar abgegrenztes elementares System, bestehend aus einer Bedrohungsquelle Q und einer Bedrohungssenke S kann somit als sicher gelten, wenn während seiner gesamten Lebensdauer $T_{Lifecycle}$ die Beziehung $R \leq R_G$ eingehalten wird, wobei natürlich stets eine gewisse Unsicherheit durch das Restrisiko verbleibt (Abb. 2), da es eine absolute Sicherheit weder in der Natur noch in der Technik gibt.

Abbildung 2: Risikoreduzierung im Zuge einer sicherheitsgerichteten Systemgestaltung [12]

Fasst man zur Verdeutlichung abschließend hierzu das derzeit hoch aktuelle Themenfeld der funktionalen Sicherheit näher ins Auge, so repräsentiert sich unter Verwendung der in Abschnitt 2 entwickelten Gedanken das entsprechende Bedrohungsszenario wie in Abb. 3 dargestellt. Das heißt, die Bedrohungsquelle ist hier das sicherheitsbezogene System selbst und Bedrohungssenke ist die von ihm zu leistende Sicherheitsfunktion. Reale Bedrohungen sind gefährliche Fehler im sicherheitsbezogenen System wie mögliches funktionelles Versagen technischer Betriebsmittel, verursacht durch Bauelemente- und Geräteausfälle, sowie Systemstörungen infolge mangelnder Zuverlässigkeit oder nicht erkannter systemimmanenter systematischer Fehler. Diese können in Form von Konstruktions-, Schaltungs-, Programmier- und Dimensionierungsfehlern oder mangelnder Funktionsstabilität gegenüber vor Ort wirkenden Beanspruchungen, aber auch durch menschliches Unvermögen, Versagen oder Fehlverhalten hervorgerufen werden. Begünstigt werden sie durch organisatorische Mängel, Missmanagement, Wissenslücken, Konzentrationsschwächen, Bedienfehler, Wartungsfehler, fehlerhafte Informationsübermittlung, Fehlinterpretation von Vorschriften oder Signalen, mangelnde Kontrolltätigkeit, Nachlässigkeit, leichtsinniger Umgang mit gefährlichen oder gefährdeten Objekten.

Funktionale Sicherheit besteht definitionsgemäß dann, wenn die Sicherheitsfunktion durch das angewandte sicherheitsbezogene System anforderungsgerecht realisiert wird. Genauer gesagt, wenn ihre Ausfallwahrscheinlichkeit, gesteuert durch ein adäquates Sicherheitsmanagement, dauerhaft einem anforderungsgerechten Sicherheits-Integritätslevel (SIL-Wert) oder Performance Level (PL-Wert) entspricht [13].

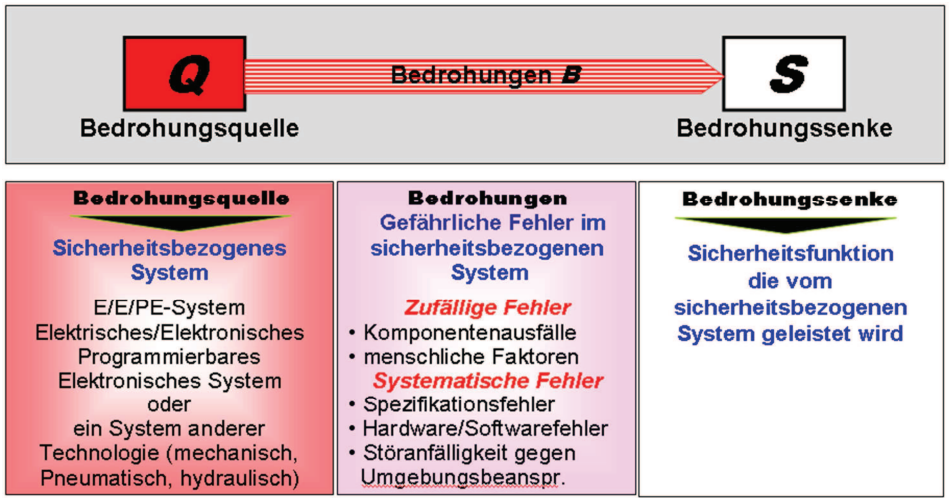

Abbildung 3: Funktionale Sicherheit – Bedrohungsszenario

Sicherheit aus systemischer Sicht

In realen industriellen Systemen (Geräte, Maschinen, Anlagen) ist für gewöhnlich nicht nur eine Bedrohungsquelle und eine Bedrohungssenke vorhanden, sondern in der Regel mehrere, die systemintern oder systemextern angeordnet und in unterschiedlichen Technologien ausgeführt sein können.

Interne Bedrohungsquellen		**Interne Bedrohungssenken**				**Externe Bedrohungssenken**			
Systemkomponenten		*K1*	*K2*	*K3*	*K4*	*S1*	*S2*		
Komponente 1	*K1*		B_1			B_2			
Komponente 2	*K2*				B_3		B_4		
Komponente 3	*K3*	B_5	B_6		B_7	B_8			
Komponente 4	*K4*								
Externe Bedrohungsquellen									
Quelle 1	*Q1*	B_9							
Quell 2	*Q2*		B_{10}						

Tabelle 3: Beispiel einer Bedrohungsmatrix, B_1 bis B_{10} Bedrohungswege

Zur Sicherstellung der Systemsicherheit sind zunächst in einer Bedrohungsanalyse die für eine bestimmte technische Anlage relevanten Bedrohungsquellen und –senken zu identifizieren und ihr sicherheitstechnisches Zusammenwirken in einer Bedrohungsmatrix darzustellen.

Danach ist für jeden Bedrohungsweg das Risiko der Schadenseintrittswahrscheinlichkeit mit technologiespezifischen Mitteln und Methoden unterhalb des Grenzrisikos zu führen und mittels eines geeigneten Risikomanagements für die

gesamte Anlagenlebensdauer dort zu halten. Tab. 3 und Abb. 4 zeigen als Beispiel die Bedrohungsmatrix und die entsprechende Struktur eines fiktiven Systems.

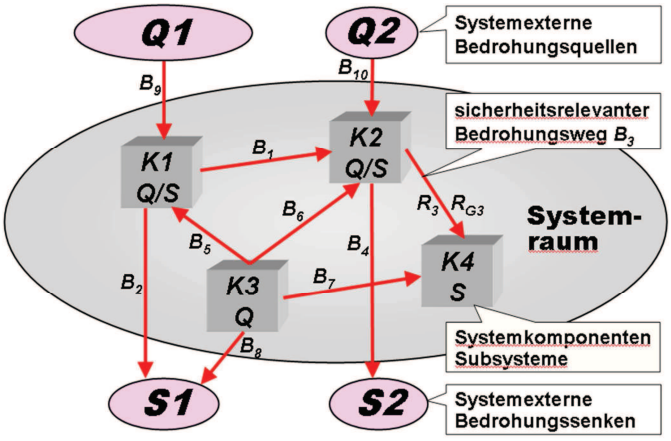

Abbildung 4: Zu Tabelle 3 adäquate Systemstruktur

***K1** bis **K4** Systemkomponenten*
***Q** Gefahrenquelle*
***S** Gefahrensenke*
***B** Bedrohungsweg*
***R** Risiko*

Ein solches System kann allgemein dann als sicher gelten, wenn durch ein leistungsfähiges Sicherheitsmanagement gewährleistet ist, dass während der gesamten Existenzphase $T_{lifecycle}$ des betrachteten Systems auf allen k sicherheitsrelevanten Bedrohungswegen $B_i \mid i \in (1, 2, \ldots, k)$ zwischen den im Zuge einer Gefahrenanalyse identifizierten Bedrohungsquellen Q und Bedrohungssenken S das jeweils wirksame Risiko $R_i \mid i \in (1, 2, \ldots, k)$ kleiner oder höchstens gleich dem jeweils zugehörigen Grenzrisiko $R_{Gi} \mid i \in (1, 2, \ldots, k)$ ist (Abb. 2).
In mathematischer Kürze: Systemsicherheit besteht, wenn folgende Bedingung erfüllt ist.

$$\textbf{Sicherheit:} \quad \forall_{B_i} (R_i \leq R_{Gi}) \text{ für alle } i \in (1, 2, \ldots, k) \text{ und } 0 \leq t \leq T_{lifecycle} \qquad (1)$$

Die Realisierung dieser Bedingung ist durch technologiespezifische Mittel und Methoden zu gewährleisten.

Bedingung (1) gilt im Übrigen nicht nur für industriell-technische Systeme sondern auch für jedes beliebige andere System.

Zusammenfassung

Sicherheit ist in einer hoch technisierten Welt ein Thema von höchster Brisanz. Ihm wird mit technologiepezifischen Maßnahmen begegnet. Das heißt die praktizierte Sicherheitstechnik und die darauf aufsetzende theoretische Behandlung sind bislang vorzugsweise nach anwendungsbezogenen Technikfeldern strukturiert, was zu vielen ähnlichen, in der Regel unscharfen, Sicherheitsinterpretationen führt. Im vorliegenden Beitrag wird die nichtfunktionale Systemeigenschaft Sicherheit unter Nut-

zung eines branchen- und technologieneutralen Quelle-Senke-Modells systemisch allgemeingültig definiert.

Literatur

[1] *Meyers Großes Universallexikon*. Bd. 13, Bibliographisches Institut Mannheim 1985, ISBN 3-411-01853-4
[2] www.duden.de/rechtschreibung/Sicherheit
[3] http://de.thefreedictionary.com/Sicherheit
[4] www.bromba.com/knowhow/sicherh.htm
[5] www.vdi.de/technik/fachthemen/technische-sicherheit
[6] www.umweltdatenbank.de/cms/lexikon/lexikon-s/1498-sicherheit.html
[7] www.kastel.kit.edu/186.php
[8] http://files.pepperl-fuchs.com/selector_files/navi/productInfo/doct/tdoct0713a_ger.pdf
[9] www.beuth.de/de/norm/din-31000-vde-1000-2011-05/139664333
[10] www.beuth.de/de/norm/din-en-61508-4-vde-0803-4-2011-02/135405992
[11] www.AuD24.net/PDF/ADK602200
[12] Habiger E.: *Sicherheit - Eine unverzichtbare Dimension im Gefüge moderner Industriegesellschaften*. Schriften der Sudetendeutschen Akademie der Wissenschaften und Künste, Bd. 31, S. 229. München 2011
[13] Habiger E.: *Openautomation Fachlexikon 2013/14*. Offenbach: 2013 VDE VERLAG GMBH