Sicherheit

Spannungsfeld Safety und Security: gestern, heute, morgen

DIANA-Sensoren zur Weichendiagnose im Stellwerk Gernsheim: Bei kritischen Infrastrukturen können sich die Sicherheit von IT-Systemen und die Sicherheit des Betriebes gegenseitig beeinflussen

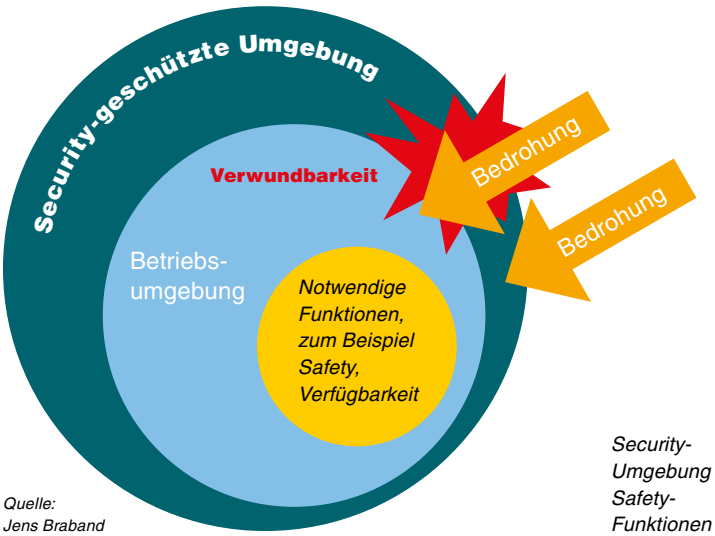
Foto: DB AG/Claudia Münchow

Dr. Jens Braband, Siemens AG, Mobility Devision, Mobility Management und Honorarprofessor der Technischen Universität Braunschweig, Institut für Eisenbahnwesen und Verkehrssicherung

Dieser Artikel beleuchtet die Wechselwirkungen zwischen Safety und Security sowohl aus technischer als auch historischer Hinsicht anhand von Beispielen aus kritischen Infrastrukturen. Um die Sachverhalte begreifbarer zu machen, wird an dieser Stelle auf das Stilmittel des Storytelling zurückgegriffen. Für vertiefte technische Betrachtungen sei auf andere Artikel verwiesen, die bereits in Deine Bahn erschienen sind (siehe Quellen am Ende des Artikels).

Es fängt schon bei der Sprache und den Definitionen an: Im Deutschen haben wir nur das eine Wort „Sicherheit" für beides, das wir dann zum Beispiel mit Adjektiven oder zu langen Wortkombinationen mit Bindestrich ergänzen. Der Einfachheit halber verwendet dieser Artikel die englischen Begriffe. Die Differenzierung erfolgt über beobachtbare Eigenschaften, die den Unterschied intuitiv näher bringen:

- Bei Safety wird in der Regel der Mensch (oder die Umwelt) vor Fehlern oder Ausfällen eines Systems geschützt, bei Security das System vor Einwirkungen des Menschen
- Safety beschäftigt sich mit unbeabsichtigten Ereignissen (beziehungsweise deren Ursachen oder Konsequenzen), Security mit beabsichtigten Ereignissen (mutwillig oder böswillig herbeigeführt)



Quelle: Jens Braband

Security-Umgebung für Safety-Funktionen

In diesem Sinn muss eine geeignete Security-Umgebung die Safety-Funktionen schützen, damit diese Mensch und Umwelt schützen können. Probleme können entstehen, wenn der Security-Schutz nicht ausreicht oder wenn die Security-Maßnahmen die Safety-Funktionen beeinträchtigen. Sowohl bei Safety und Security sind in der Regel systematische Fehler die Ursachen für die meisten Probleme, bei Safety führt dies dazu, dass die Schutzfunktion nicht erbracht wird, bei Security dazu, dass der Schutz vor äußeren Einwirkungen Schwächen enthält, die ein Angreifer ausnutzen kann.

In diesem Artikel wird unter „System“ in der Regel ein technisches System verstanden (gegebenenfalls mit Bediener) und „Safety“ wird als Betriebssicherheit beziehungsweise funktionale Sicherheit verstanden. Unter „Security“ wird bei einem technischen System hier vorwiegend die IT-Sicherheit verstanden (gegebenenfalls inklusive physischer Effekte).

Ein Beispiel

Um das grundsätzliche Spannungsfeld zu beleuchten, betrachten wir die Cockpit-Tür in einem zivilen Verkehrsflugzeug als System. Dabei handelte es sich historisch um ein physisches System, das aber seit längerem durch elektronische Komponenten erweitert wurde.

Vor den Terroranschlägen des 11. September 2001 war die Cockpit-Tür in der Regel unverschlossen und es war bei Passagieren beliebt, bei längeren Flügen mal ins Cockpit schauen zu dürfen. Hier war der Schwerpunkt Safety und Security, von Ausnahmefällen abgesehen, eher untergeordnet. Dies änderte sich danach abrupt und die Cockpit-Tür musste von innen verschlossen werden. Security bekam also die Oberhand und Safety schien dadurch gesichert, dass immer zwei Piloten im Cockpit waren. Dann endete Helios-Airways-Flug 522 am 14. August 2005 mit einem Totalverlust. Die Ursache bestand unter anderem darin, dass in Folge eines Druckabfalls beide Piloten bewusstlos wurden und die Crew wegen der verschlossenen Cockpit-Tür nicht beziehungsweise erst zu spät eingreifen konnte: Die Security beeinträchtigte die Safety.

Cockpit-Tür eines zivilen Verkehrsflugzeugs

Foto: Thilo Parg/Wikimedia Commons, Lizenz: CC BY-SA 4.0

Danach wurden die Cockpit-Türen umgerüstet und erhielten in der Regel ein elektronisches Schloss, bei dem eine Öffnung von außen mit einer PIN angefordert werden kann. Dies kann aber vom Piloten für einen definierten Zeitraum pro Anforderung, zum Beispiel fünf Minuten, übersteuert werden. Scheinbar ein guter Kompromiss zwischen Safety und Security – bis zu Germanwings-Flug 9525, bei dem am 24. März 2015 ein Pilot in Selbstmordabsicht die Maschine zum Absturz gebracht haben soll.

Problematisch war, dass sich ein einzelner Pilot im Cockpit einschließen konnte. Daraufhin wurde bei den meisten Fluggesellschaften die Regel eingeführt, dass immer mindestens zwei Personen im Cockpit sein müssen, das heißt, ein weiteres Besatzungsmitglied muss einen Piloten ersetzen, wenn er das Cockpit verlässt. Ob dies auf Dauer zielführend ist, wird sich zeigen. Zusammengefasst zeigt dieses Beispiel die komplexen Wechselwirkungen zwischen Safety und Security, bei denen es unter Umständen nicht möglich ist, alle Anforderungen vollständig umzusetzen. Ziel muss sein, unter Berücksichtigung von Safety und Security eine optimierte Gesamtlösung zu finden, die das Gesamtrisiko minimiert.

Safety und Security gestern

Im Dezember 2017 wurde ein weiterer Teil der Schnellfahrstrecke Nürnberg–Erfurt auf Basis der Spezifikationen nach dem European Train Control System (ETCS) in Betrieb genommen, für die die Grundlagen in den Bereichen Safety und Security bereits Mitte der 1990er-Jahre abgestimmt wurden.[1] Deswegen lohnt sich ein Blick in den Rückspiegel.

Wenn wir in die frühen 1990-er Jahre zurückkehren könnten, was würde uns technologisch auffallen? Die GSM-Netze D1 und D2 sind gerade in Betrieb gegangen, die Handys haben deutlich erkennbare Antennen. Windows 3.1 ist das aktuelle PC-Betriebssystem. Computerviren sind zwar seit 1986 bekannt, betreffen aber vor allem DOS. Michelangelo ist das erste Virus, das durch die Medien der breiten Öffentlichkeit bekannt wird. 1992 wird der erste kommerzielle Internet-Provider in Deutschland gegründet. 1993 wird der erste Webbrowser namens Mosaic veröffentlicht. In Deutschland gibt es etwa 15 Webserver und bei der Deutschen Bundesbahn (!) wurden gerade die ersten Serien-ESTW (elektronische Stellwerke) in Betrieb genommen, viele davon entlang der 1991 fertiggestellten Neubaustrecke Hannover–Würzburg. Das Bundesamt für Sicherheit in der Informationstechnik war 1991 gegründet worden und das Eisenbahn-Bundesamt (EBA) ging 1994 aus dem Bundesbahn-Zentralamt (BZA) hervor.

Schon damals war es notwendig, im Sicherheitsnachweis nach den Technischen Grundsätzen für die Zulassung von Sicherungsanlagen des EBA (Mü8004) den Betrieb unter externen Einflüssen zu betrachten. Dazu gehörte auch unberechtigter Zutritt beziehungsweise Zugriff. Zugegebenermaßen lag der Fokus auf physischem Zugriff und der Nachweis erfolgte weitgehend regelbasiert, nicht risikobasiert. Nur wenn das System grundlegend verändert wurde, wurden Risikobetrachtungen notwendig, um neue Regeln zu schaffen. Die wesentliche Änderung der Linienzugbeeinflussung (LZB) zu ETCS war die Einführung der Funkzugbeeinflussung, deren Auswirkungen auf Safety und Security sehr ausführlich untersucht wurde. Hier sollen nur einige grundsätzliche Aspekte dargestellt werden.

Mit dem Mobilfunkstandard GSM-R wurde ein kommerzielles Funksystem eingeführt, auf das unberechtigter Zugriff nicht ausgeschlossen werden kann. Also war von Anfang an klar, dass die Datenübertragung kryptographisch gesichert werden muss. Die Frage, wo die Sicherung und Prüfung erfolgen sollte, wurde intensiv diskutiert. Aus Security-Sicht bot GSM-R Verschlüsselungsmechanismen an. Aber aus Safety-Sicht stellte sich die Frage, wie diese Funktionalität im Betrieb geprüft werden kann. Außerdem war fraglich, ob eine Sicherung nur im Kommunikationsnetzwerk ausreichen würde. Schließlich setzte sich Safety mit einer eigenen Ende-zu-Ende-Sicherung vom Radio Block Center (RBC) zum Fahrzeuggerät durch. Zum Glück, kann man im Nachhinein sagen, denn schon ab 2000 galten wesentliche Varianten des Verschlüsselungsalgorithmus A5 des GSM als nicht mehr hinreichend sicher und spätestens seit dem Bekanntwerden des SS7-Hack 2014 ist die Security des gesamten GSM bis hin zum modernsten Mobilfunkstandard UMTS fraglich.

Aber auch früher gab es schon Konflikte zwischen Security und Safety. Damals dauerte die Prüfung eines kryptographischen Codes relativ lange, je nach Rechner bis zu mehreren Sekunden. Dies erschien für Nothaltanforderungen aus Safety-Sicht inakzeptabel, so dass auf eine kryptographische Sicherung solcher Nachrichten verzichtet wurde. Dies bedeutet aus Security-Sicht, dass jeder, der Zugriff auf das Kommunikationsnetz hat, Nothalte einspielen könnte, was aber aus Safety-Sicht nur betriebseinschränkend wirkt.

Aus heutiger Sicht sind die kryptographischen Sicherheitsmechanismen zwar vernünftig entwickelt worden, aber eben gegen die Anforderungen von vor 25 Jahren. Zum Beispiel wird der verwendete 3DES-Algorithmus heute für neue Systeme nicht mehr empfohlen, genauso wie die effektive Schlüssellänge von 112 Bit. Das heißt, anders als bei der Safety üblich, haben die Security-Anforderungen eine begrenzte Lebensdauer und müssen regelmäßig überprüft und angepasst werden. Dies bedeutet, dass für ETCS aus Security-Sicht in etwa 10 bis 20 Jahren ein Re-Design der Sicherungsverfahren notwendig wird, während dies aus Safety-Sicht nicht notwendig wäre.

Diese Beobachtungen lassen sich verallgemeinern, denn überall, wo maßgebliche Änderungen vorgenommen wurden, wurden zusätzliche Security-Betrachtungen durchgeführt, denn auch die Norm EN 50129 als Nachfolger der Mü8004 auf europäischer Ebene hat das Prinzip des Sicherheitsnachweises übernommen.

Safety und Security heute

In den letzten Jahren hat sich die Lage komplett geändert. Ging es früher um einzelne Änderungen beziehungsweise Einführung einzelner neuer Technologien, wie zum Beispiel GSM, so werden in den letzten Jahren immer mehr neue Technologien, zum Teil gleichzeitig, eingeführt, deren Security- und Safety-Auswirkungen analysiert werden müssen. Dabei besteht insbesondere in jüngster Zeit das Problem, dass Systeme gehackt werden und dabei grundsätzliche Security-Annahmen in Frage gestellt werden.

Im Bereich der Rechnertechnik geht der Trend immer mehr zu kommerziellen Betriebssystemen und zur Miniaturisierung beziehungsweise Virtualisierung, das heißt, es sollen – strikt voneinander getrennt – mehrere Prozesse auf einem Rechner ausgeführt werden, zum Beispiel Safety- und Nicht-Safety-Anwendungen. Die Trennung wird von spezieller Software (SW), häufig Hypervisor genannt, sichergestellt, oft auch vom Betriebssystem selbst. Durch die im Juli 2017 entdeckten, aber erst dieses Jahr veröffentlichten Sicherheitslücken Meltdown beziehungsweise Spectre wird aber genau dieser unautorisierte Zugriff auf fremde Speicherbereiche ermöglicht, und zwar praktisch auf allen modernen Prozessoren. Dies mag zunächst wie ein reines Security-Problem aussehen, da Speicherbereiche nur ausgelesen, aber nicht manipuliert werden können. Allerdings könnten im kompromittierten Speicher Passwörter stehen, die wiederum Zugriff auf Safety-Prozesse erlauben. Da hier aber eine direkte SW-Ausführung auf den Zielsystemen stattfinden muss, ist das Safety-Problem eher gering: Bei Rechnern, auf denen Safety-Prozesse laufen, werden in der Regel auch die anderen Prozesse bei der Zulassung geprüft und ein Nachladen von Schad-SW dadurch erschwert.

In der Kommunikationstechnik sind nach GSM weitere Systeme, wie zum Beispiel WLAN (IEEE 802.11), gebrochen worden. Der KRACK-Hack zeigte 2017, dass es möglich ist, WPA2-Schlüssel zu kompromittieren. Bemerkenswert ist hier, dass das Handshake-Protokoll zum Aushandeln der Schlüssel sogar als mathematisch korrekt bewiesen wurde. Der Beweis ist zwar richtig, aber die Hacker haben sich einfach nicht an die Annahmen des Beweises gehalten. Dieser Hack kann auch Safety-Auswirkungen haben, wenn man sich alleine auf die Security des WLAN verlässt.

Auch für Satelliten-Navigationssysteme wie GPS sind Angriffe bekannt. Zum Beispiel können durch Spoofing (Täuschungsmethode in Computernetzwerken zur

WLAN-Nachrüstung in ICE der Deutschen Bahn: Der Einbruch in gesicherte Systeme der Kommunikationstechnik (Security-Problem) kann Konsequenzen für die Safety haben

Vortäuschung einer anderen Identität) formal gültige, aber falsche Positionsdaten erzeugt und im GPS-Format übertragen werden. Dadurch ist es bereits gelungen, Schiffe oder Drohnen vom Kurs abzubringen. Nur für militärische Anwendungen werden die Daten verschlüsselt übertragen. Für GPS gibt es für zivile Anwendungen wenige Lösungen, außer eventuell speziell gerichtete Antennen. Dies bedeutet, dass es erhebliche Safety-Probleme mit sich bringen kann, wenn man sich alleine auf GPS stützt. Die kommerziellen Dienste von Galileo sollen allerdings eine Authentifizierung der Signale ermöglichen.

Und zu guter Letzt muss natürlich noch WannaCry erwähnt werden, eine Ransomware, die einen Fehler in einem Microsoft-Protokoll ausnutzte, der Geheimdiensten schon seit Jahren bekannt war. Zwar gab es für dieses Problem bereits seit März 2017 einen Patch (Nachbesserung von Software), aber trotzdem wurden im Mai 2017 noch über 230.000 Rechner weltweit infiziert, darunter auch Fahrgastinformations- und Leitsysteme bei der Deutschen Bahn (DB). Das Problem bestand darin, dass die Systeme entweder nicht rechtzeitig aktualisiert wurden oder dass für ältere Betriebssysteme keine Patches mehr bereitgestellt wurden. Dies war zwar kein Safety-Problem, aber aus Security-Sicht bestand eine erhebliche Beeinträchtigung der Verfügbarkeit.

Schließlich kann man sich noch fragen, ob aus solchen Security-Problemen heute überhaupt schon Safety-Probleme entstanden sind. Zumindest für Bahnsysteme sind bis heute keine Fälle veröffentlicht worden. Man kann den Fokus aber etwas erweitern auf industrielle Steuerungssysteme in kritischen Infrastrukturen, die am ehesten mit Bahnsystemen vergleichbar sind.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat schon 2016 berichtet, dass nach einem Cyber-Angriff ein deutsches Stahlwerk abgeschaltet werden musste, bevor es zu Schäden kommen konnte. Schwachstellen wurden außerdem in Fernwartungssystemen von Industrieanlagen, zum Beispiel Wasserwerken, aber auch Verkehrssystemen wie Baustellen-Ampelanlagen, gefunden, mit denen die Anlagen hätten manipuliert werden können. Das BSI schätzt derzeit kritische Infrastrukturen als „lohnendes Ziel“[2] ein, insbesondere für politisch oder kriminell motivierte Angreifer.

Der grundsätzliche Erkenntnisgewinn aus diesen und vielen anderen Fallbeispielen besteht darin, dass sich im Gegensatz zur Safety bei der Security die Lage ganz kurzfristig ändern kann, obwohl man sich in der Regel an Standards und Best Practices gehalten hat. Dies liegt einerseits an der Komplexität und Vielzahl der Schnittstellen und Systeme, die niemals fehlerfrei sind, und andererseits an dem Einfallsreichtum, man darf fast sagen der Genialität, der Angreifer, die zum Beispiel bei KRACK oder Meltdown/Spectre bisher nicht für möglich gehaltene Wege gefunden haben. Dies bedeutet aus Safety-Sicht, dass man sich zwar auf die gute Arbeit der Security-Kollegen verlassen darf und sollte, aber jederzeit damit rechnen muss, dass zumindest ein Security-Mechanismus (teilweise) umgangen werden kann. Man ist also gut beraten, dem Defense-in-depth-Prinzip zu folgen und sich nicht alleine auf die Wirksamkeit einer einzelnen Maßnahme zu verlassen. Dies entspricht vom Ansatz her dem Safety-Prinzip, dass der erste Ausfall ungefährlich sein muss. In beiden Fällen muss man allerdings die Verwundbarkeit (Security) beziehungsweise den Ausfall (Safety) so früh wie möglich erkennen, um das Problem dann in einer gewissen Zeit entweder zu patchen (Security) beziehungsweise zumindest den sicheren Zustand einzunehmen (Safety).

Safety und Security morgen

Schon Mark Twain wusste, dass „Prognosen eine schwierige Sache [sind], vor allem, wenn sie die Zukunft betreffen“. Damit hat er sicherlich Recht, aber ein paar Trends sind unübersehbar.

Zunächst werden immer komplexere Systeme auch in der Eisenbahn genutzt werden, ob das nun Fibre Optical Sensing, Künstliche Intelligenz oder Cloud-Dienste sein mögen, und sie werden auch für Anwendungen genutzt werden, die für Safety relevant sind. Dazu gehört auch die Kommunikation über IP-Technologien, die wesentlicher Bestandteil des neuen sogenannten digitalen Stellwerks der DB sind.

Dies stellt enorme Anforderungen an das System Engineering, das auch ein umfassendes Security Engineering beziehungsweise Management nach anerkannten Standards wie zum Beispiel IEC 62443 umfassen muss. Außerdem werden kritische Security-Komponenten oder Dienste von qualifizierten Prüfstellen zertifiziert werden müssen, sei es von unabhängigen Organisationen innerhalb oder außerhalb von Betreibern oder Herstellern.

Trotz aller Anstrengungen muss man mit plötzlich aufgedeckten Schwachstellen rechnen und Notfall-Teams (CERT) einrichten, die schnell und kompetent handeln. Hier kommt insbesondere dem Erkennen von Schwachstellen oder Anomalien (dem Monitoring) eine besondere Bedeutung zu, genauso wie den Prozessen des raschen SW-Updates.

Eine ganz besondere Rolle werden dabei die Mitarbeiter spielen, denn bei vielen gezielten Angriffen, den sogenannten Advanced Persistent Threats, ist es notwendig, zunächst einmal Zugriff zu einem System zu erlangen (physisch und logisch) und dazu braucht man Zugriffsrechte. Das kann zum Beispiel durch das Brechen schwacher Passwörter erfolgen, aber auch durch gezieltes Ausspähen und Installation von Malware (Phishing). Hier bedarf es eines besonderen Bewusstseins der Mitarbeiter sowie einer geeigneten Unternehmenskultur, ja einer speziellen Security-Kultur als Teil der Sicherheitskultur[3], damit die Mitarbeiter einerseits den Security-Regeln folgen, andererseits aber auch bei Abweichungen und Anomalien ein gesundes Misstrauen besitzen (im Sinne von Gefahrenbewusstsein).

In diesem Sinn passt hier ein Zitat des französischen Schriftstellers Victor Hugo: „Für Schwache ist [die Zukunft] das Unerreichbare, für die Furchtsamen das Unbekannte, für die Mutigen die Chance." Auch für das System Bahn sollten die Chancen der Digitalisierung mutig genutzt werden, allerdings nicht ohne eine sorgsame und umsichtige, vielleicht sogar furchtsame Analyse des heute noch Unbekannten, das heißt mit angemessenem Respekt vor den Risiken, mit dem wir in der Security in Zukunft konfrontiert werden. Gelingt dies nicht, so wird die Vision der Digitalisierung von kritischen Infrastrukturen unerreichbar bleiben.

Zusammenfassung

In der Eisenbahnsignaltechnik spielt Security, insbesondere hinsichtlich des Einflusses auf Safety, schon lange eine Rolle und wird auch im Sicherheitsnachweis betrachtet, zumindest die Rückwirkungsfreiheit. Bisher wurde Security vor allem bei größeren Änderungen an bestehenden Systemen ausführlich betrachtet, insbesondere bei neuen Kommunikationstechnologien. Diese Betrachtungen müssen zukünftig erweitert werden und sollten auf Grundlage internationaler Standards wie IEC 62443 erfolgen.

Die in Zukunft im Zuge der Digitalisierung auch bei der Eisenbahn eingesetzten Systeme werden immer leistungsfähiger und komplexer. Dadurch entstehen weitere Herausforderungen für das Spannungsfeld Security und Safety, das bereits heute besteht, und für das manchmal keine optimalen Lösungen gefunden werden können, aber tragbare Kompromisse. In Zukunft ist neben den technischen Lösungen besonderes Augenmerk auf das Monitoring, das Patching sowie die Ausbildung beziehungsweise Erhaltung einer Sicherheitskultur zu legen. Ganz klar ist allerdings, dass Digitalisierung ohne Safety und Security scheitern wird. ■

Abkürzungen

BS	Bundesamt für Sicherheit in der Informationstechnik
CERT	Computer Emergency Response Team
DES	Data Encryption Standard
DOS	Disk Operating System
ESTW	Elektronisches Stellwerk
ETCS	European Train Control System
GSM	Global System for Mobile Communication
GPS	Global Positioning System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IT	Informationstechnik
KRACK	Key Reinstallation Attack
LZB	Linien-Zugbeeinflussung
PIN	Persönliche Identifikationsnummer
SS7	Signalling System 7
UMTS	Universal Mobile Telecommunication System
WLAN	Wireless Local Area Network
WPA2	Wi-Fi Protected Access 2

Quellen

[1] Braband, J.: EURORADIO: Verläßliche Übertragung sicherheitsrelevanter Zugbeeinflussungsdaten über offene Netzwerke. In: H. H. Brüggemann und W. Gerhardt-Häckl (Hrsg.): Verläßliche IT-Systeme VIS'95, Vieweg, Braunschweig, 1995, 297–306.

[2] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2017.

[3] Braband, J.: Sicherheitskultur – Schlüsselrolle für die Sicherheit des Systems Bahn, Deine Bahn, 11/2011, 12–17.

[4] Bock, H., Braband, J.: Safety Integrity und Security Level – zwei Seiten derselben Münze?, Deine Bahn, 6/2014