Safety and Security

Thomas Jäger

Department Informatik
Hochschule für Angewandte Wissenschaften Hamburg
Berliner Tor 7
20099 Hamburg
thomas.jaeger@haw-hamburg.de

Abstract. Diese Arbeit behandelt die Verschmelzung zweier bisher weitgehend getrennt betrachteter Teilbereiche der IT-Sicherheit: Safety und Security. Zunächst wird eine Abgrenzung und Erklärung der Begriffe vorgenommen, um anschließend deren Zusammenwachsen zu erläutern und mit Hilfe von Beispielen zu konkretisieren. Desweiteren werden die daraus entstehenden Herausforderungen aufgezeigt und anhand verschiedener Paper beispielhaft bereits vorhandene Lösungsansätze skizziert. Ein Blick auf aktuelle Konferenzen zum Thema machen die bereits vorhandene und stetig wachsende Relevanz und Brisanz der Thematik deutlich. Im Zuge dessen wird abschließend ein Ausblick auf zukünftige Entwicklungen und mögliche Vorgehensweisen in Bezug auf das Testen von safety- und security-relevanten Fälle gegeben.

1 Einleitung

Das rasante Fortschreiten der Digitalisierung und Vernetzung unserer Gesellschaft und der Welt bietet immer bessere, schnellere, vor wenigen Jahren noch kaum vorstellbare Möglichkeiten und Vorteile. Nicht nur industrielle und wirtschaftliche Bereiche sind betroffen, auch das private Leben wird immer stärker von neuen Geräten, Methoden und Möglichkeiten durchdrungen, die das vermeintliche Ziel haben, das Leben und den Alltag leichter, schneller und komfortabler zu gestalten. Allerdings: je mehr Verantwortung in die Hände von Software, Computern und Maschinen gelegt wird, desto größer werden Risiken und desto verletzlicher machen wir uns gegenüber Gefahren, die aus dem Umgang mit selbigen entstehen können.

Durch die beschriebenen Entwicklungen beginnen ursprünglich getrennte Bereiche der Informatik miteinander zu verschmelzen. Aus dieser Kombination entstehen neue Risiken, die schwerer zu erfassen sind. Die beiden Teilbereiche Safety und Security stellen einen solchen Fall dar. Bezeichnen sie zunächst einen einfachen deutschen Begriff, "Sicherheit", sind sie in ihrer Bedeutung, dem durch sie beschriebenen Gefahrenpotential und den Methoden zu dessen Bekämpfung, grundlegend verschieden.

1.1 Safety

Eine gute Herangehensweise, um den Begriff Safety verstehen zu können, ist es, zunächst klar zu machen, was die Risiken sind, die von safety-kritischen Systemen ausgehen können. Generell ist ein safety-kritisches System ein System, welches das Potential hat, seiner Umwelt physisch oder materiell zu schaden. Hierzu zählen Personen- und Sachschäden sowie ökologische und finanzielle Schäden. [7] Safety-kritische Systeme waren traditionell von der informatischen Außenwelt isolierte Systeme, was bedeutet, dass sie in sich geschlossen keine Verbindungen/Schnittstellen zu anderen Softwaresystemen hatten. Beispiele hierfür sind industrielle Produktionsmaschinen, ebenso wie Autos und Kraftwerke, aber auch medizinische Geräte, die für das Überleben von Patienten notwendig sind.

Safety Engineering beschreibt Maßnahmen die ergriffen werden, um die Wahrscheinlichkeit einer Schädigung der Umwelt zu verringern, abzuschwächen oder idealerweise zu verhindern, indem systeminterne Fehlfunktionen verhindert oder deren Auswirkung abgefedert oder begrenzt werden. Um Security-Aspekte, auf die im folgenden Abschnitt näher eingegangen wird, zu begegnen, werden meist nur Offline-Maßnahmen ergriffen (Passwörter, Schlüssel, etc.).

1.2 Security

Security-kritische Systeme sind von Haus aus nicht-isolierte Systeme, die Daten mit anderen Systemen über Schnittstellen austauschen. Hierzu zählen beispielsweise Netzwerke jeglicher Art (insbesondere Firmen- oder andere vertrauliche Netzwerke, da hier mehr Schaden verursacht werden kann), Clouds und Software für Finanzdienstleistungen. Auch hauptsächlich privat genutzte Systeme wie Smartphones, soziale Netzwerke, etc. müssen mitbetrachtet werden. Die potentiellen Gefahren für security-kritische Systeme sind der Datenverlust, die Manipulation von Daten sowie der Datendiebstahl. Somit stellen sie, im Gegensatz zu den safety-kritischen Systemen, keine Gefahr für ihre Umwelt dar, sondern benötigen Schutz vor dieser. [7] Mit Maßnahmen wie der teilweisen Isolation von Systemen oder Komponenten durch Authentifizierungsmechanismen und kryptographischen Verfahren darum, die Sicherheit security-kritischer Systeme aufrecht zu erhalten.

1.3 Safety + Security

Durch die Digitalisierung und die damit einhergehende rasante Ausbreitung des Internets nimmt die Verbreitung safety-kritischer Komponenten zu, welche nicht mehr isoliert und in sich geschlossen existieren und funktionieren, sondern miteinander oder der Außenwelt vernetzt agieren. Dadurch entstehen Schnittstellen zwischen verschiedenen Systemen oder Komponenten, die folglich eine potentielle Angriffsfläche für Attacken von außen darstellen. Somit kann eine Situation herbeigeführt werden, in der ein safety-kritisches System eine Fehlfunktion, einen Ausfall oder andere Störungen erleidet, die vorsätzlich von einem Angreifer außerhalb des Systems ausgelöst wurde. Arbeitet man weiterhin lediglich

mit herkömmlichen Safety-Methoden um Fälle wie diese zu verhindern, könnte die Kontrolle über die Integrität des Systems verloren gehen. [6]

1.4 Beispiele

Um die Relevanz und Verbreitung dieser Verschmelzung zu erfassen ist es wichtig, einige bereits existierende Beispiele zu betrachten. Hier ist der Verkehr, im Speziellen der Luftverkehr anzuführen, den Nadja Menz, Petra Hoepner, Jens Tiemann und Frank Koußen in ihrer Veröffentlichung "S2: Safety und Security aus dem Blickwinkel der öffentlichen IT"[7] beschreiben. In der Luftfahrt sind die Aufgaben zur Gewährleistung der Sicherheit klar in zwei Aufgabenbereiche geteilt: Air Safety und Air Security. Während sich Air Safety mit inneren Gefahren und Gefahren für die öffentliche Sicherheit beschäftigt, kümmert sich die Air Security um solche, die von außen auf das Flugzeug einwirken. Nun könnte es passieren, dass im Übergangsbereich der beiden Aufgabenfelder eine Grauzone und dadurch Risikoszenarien entstehen, die außer Acht gelassen werden. Vorstellbar wäre ein Angriff von außen auf die Systeme des Flugzeugs, um diese so zu manipulieren, dass sich eine Turbine überhitzt oder durch einen Eingriff ins Steuersystem die Flugroute ändert und das Flugzeug so zum Absturz gebracht oder entführt werden kann. Eine ähnliche Gefährdung ist mittlerweile aber nicht nur in großen Verkehrsmaschinen wie Flugzeugen oder in der Raumfahrt denkbar, sondern auch im normalen Straßenverkehr und privaten Automobilen. Auf diesen Fall wird später genauer eingegangen.

Eines der bekanntesten Beispiele, auch wenn nicht als Safety & Security Fall bekannt, ist der Virus Stuxnet. Hier wurde durch ein eingeschleustes Schadprogramm die Geschwindigkeit der Zentrifugen einer Atomanlage des Iran manipuliert. Diese wurden dadurch beschädigt und die Anreicherung von Uran verlangsamt. Darüber hinaus könnten auf diesem Wege weitaus schlimmere Unfälle innerhalb eines solchen Kraftwerkes verursacht oder die Stromversorgung der von diesem Kraftwerk abhängigen Infrastruktur beeinträchtigt werden oder ausfallen. Übertragungsweg war möglicherweise ein USB-Stick. Dieser Fall lässt erkennen, dass die Thematik auch politische Relevanz haben kann.[7]

Auch auf dem Gebiet der medizinischen Implantate, in diesem Fall ein Herzschrittmacher, spielt die Verschmelzung von Safety und Security eine Rolle. So hat Marie Moe und Eireann Leverett von der unabhängigen Forschungsorganisation SINTEF in Norwegen ihren eigenen Herzschrittmacher (ein safetykritisches System) auf Schnittstellen und mögliche Angriffspunkte, die ins Aufgabenfeld der Security fallen, untersucht. Dabei wurden kabellose Schnittstellen wie eine Bluetooth-Anbindung entdeckt, über die Ärzte bei Fehlfunktionen Updates auf den Herzschrittmacher spielen können, um Probleme zu beheben. Denkbar wäre aber auch, dass sich ungebetene Personen Zugang verschaffen, um das Gerät zu manipulieren. Welche möglichen Konsequenzen im schlimmsten Fall daraus resultieren könnten, ist leicht vorstellbar und hochgefährlich.[8]

2 Herausforderungen

Resultierend aus der Verschmelzung dieser beiden Bereiche, Safety und Security, müssen Schlussfolgerungen gezogen und über Konsequenzen nachgedacht werden. Einen Anfang machen Andrew J. Kornecki von der Embry Riddle Aeronautical University und Janusz Zalewsky von der Florida Gulf State University in ihrem 2010 veröffentlichten Paper "Safety and Security in Industrial Control"[6], in dem sie entstehende Probleme und Herausforderungen aufzeigen. Auch Nadja Menz, Petra Hoepner, Jens Thiemann und Frank Koußen nehmen sich der Thematik in ihrem 2015 veröffentlichten Whitepaper "S2: Safety und Security aus dem Blickwinkel der öffentlichen IT"[7] an.

Beide Paper zeigen, dass eines der grundlegendsten Probleme ist, dass Safety und Security als zwei voneinander getrennte Bereiche betrachtet werden. Um der Herausforderung begegnen zu können, müssen beide Bereiche zum Schutz von Systemen ebenso miteinander verwoben werden, wie es die potentiellen Gefahren sind. Durch die Integration mehrerer Systeme oder Komponenten entstehen Kommunikations- und Netzwerkschnittstellen, was dazu führt, dass safety-kritische Systeme nicht mehr durch Isolation vor Attacken auf der Security-Ebene geschützt sind. Diese Vernetzung von Systemen oder Komponenten erhöht zugleich die Komplexität des dadurch entstehenden Systems. Mit steigender Komplexität steigt die Wahrscheinlichkeit zur Häufung von Fehlfunktionen und Schwachstellen. Vernetzt man zwei in sich sichere Systeme miteinander, ist dies keine Garantie dafür, dass ein sicheres Gesamtsystem entsteht. Vielmehr kann Vernetzung Sicherheitslücken aufreißen, wo vorher keine waren. Besonders verwundbare Schnittstellen können sich dann auftun, wenn Systeme oder Komponenten über immer stärker verbreitete kabellose Verbindungen miteinander kommunizieren. Eine weitere Gefahr der wachsenden Komplexität von Systemen ist es, dass bereits kleine Fehlfunktionen in Teilsystemen unvorhersehbare und unkalkulierbare Ereignisse im Gesamtsystem auslösen können.[7]

Auch werden große Lücken in der Ausbildung von Fachkräften erwähnt. Zum Einen ist festzustellen, dass Security-Spezialisten weder mit Safety-Richtlinien oder Problematiken vertraut sind, genauso wenig wie sich Safety-Experten auf das Gebiet der Security verstehen. Zum Anderen besteht eine Wissenslücke bei Fachkräften und in Unternehmen über die Existenz dieser neu aufkommenden Safety und Security Problematik, geschweige denn der Konsequenzen und Maßnahmen, die daraus gefolgert werden müssten. Entgegentreten kann man dieser Problematik nur mit konsequentem Austausch und konstruktiver Zusammenarbeit verschiedener Expertengruppen. [6]

3 Lösungsansätze

Um den Herausforderungen zu begegnen, wurden bereits verschiedene Ansätze entwickelt, die sich genau mit diesem neuen Aufgabengebiet beschäftigen. Diese basieren auf zum Teil grundlegend verschiedenen Denk- und Vorgehensweisen. Zwei dieser Beispiele werden in diesem Kapitel beschrieben und auf ein drittes hingewiesen.

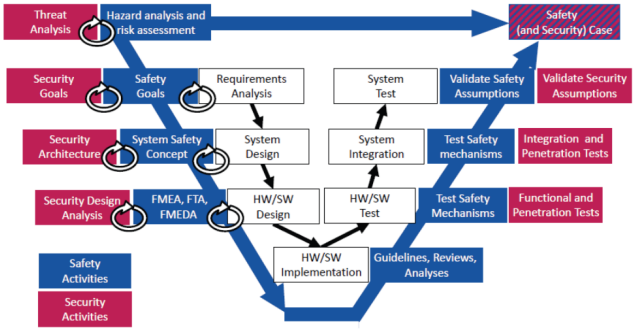
3.1 Automotive Functional Safety + Security

Simon Burton von der ETAS GMBH, Jürgen Likkei und Priyamvadha Vembar von der Robert Bosch GmbH und Marko Wolf von der ESCRYPT GmbH haben sich diesem Thema in ihrem 2012 veröffentlichten Paper "Automotive Funtional Safety + Security" [4] genähert. Das Umfeld, in dem sich diese Arbeit bewegt, ist die Automobilindustrie, in der eine immer größere Anzahl von miteinander und mit der Außen- und Umwelt kommunizierenden Komponenten in Fahrzeugen verbaut wird, insbesondere auch in Hinblick auf zukünftige Entwicklungen autonom gesteuerter Autos. Damit tun sich Security-Lücken in einem eigentlich safety-kritischen System auf. Das Risiko, dass ein Angriff von außen zu Fehlfunktionen im Auto führt, soll verringert werden. In schlimmsten Fällen könnte das dazu führen, dass der Fahrer die Kontrolle über sein Fahrzeug verliert und somit bewusst Unfälle herbeigeführt werden können. Dazu könnte der Angreifer versuchen, Falschmeldungen an den Spurhalteassistenten zu senden, der im normalen Betrieb auslöst, wenn der Fahrer die Spur verlässt. Das Einschleusen solcher gefälschter Nachrichten könnte beispielsweise über die Kamera des Autos erfolgen. Die möglichen Folgen wären ungewollte Warnungen, ungewollte Steuerung und Ausweichmanöver. Das ein externes Eingreifen auf solchen Wegen in der Praxis bereits möglich ist, zeigte der ADAC in einer Studie vom Januar 2015 an BMW Fahrzeugen bei der es gelang, Fahrzeuge per Mobilfunk zu ffnen, ohne Spuren zu hinterlassen. Weitere Manipulationen wurde im Zuge dieser Studie nicht vorgenommen, wären aber ebenso denkbar gewesen.[2]

Idee Die Grundidee dieses Ansatzes ist es, ein klassisches Entwicklungsmodell, konkret das V-Modell, um Safety und Security-Anteile zu erweitern. Hierzu wird angedacht, ISO 26262 [12] und ISO 14508 [11] miteinander zu kombinieren. ISO 26262 stellt den Safety-Anteil, beschreibt den "International standard for functional safety in passenger vehicles" und hat zum Ziel, die Risiken durch System- und Hardwarefehler zu minimieren. Dabei werden herkömmliche Analysemethoden wie die Fault Tree Analysis oder Failure Mode and Effects Analysis während der Konzeptionierungsphase verwendet und die entsprechenden Tests zur Überprüfung der safety-relevanten Anteile während der Testphasen eingebaut. Der Security-Anteil dieses Ansatzes soll von ISO 14508 abgedeckt werden, welches aus einem Katalog herkömmlicher Securityanforderungen besteht. Die Verfasser des Papers fügen diese Anforderungen zu den Aspekten aus ISO 26262 hinzu und erhalten das auf Fig. 1 sichtbare erweiterte V-Modell.

Nun ist es in diesem Ansatz vorgesehen, dass auf Basis der durch Gefährdungsanalyse und Risikoabschätzung (Hazard Analysis und Risk Assessment) aus ISO 26262 entwickelten Safety-Ziele die Security-Ziele konzeptioniert werden. Dadurch wird nach der Frage gearbeitet, ob Safety-Ziele vorhanden sind, die durch Angriffe von außen gefährdet werden könnten. Aus Basis dieser erarbeiteten Safety und Security-Zielen könnten in der Testphase des Projekts folglich Testfälle und Testziele entwickelt werden.

Fig. 1. Erweitertes V-Modell



Quelle: Simon Burton and Jürgen Likkei and Marko Wolf: "Automotive Functional = Safety + Security" [4]

Eindruck Einerseits liefert der Ansatz gute Grundgedanken, da er althergebrachte Entwicklungszyklen um die Aspekte erweitert, die zur Sicherstellung der Sicherheit des entstehenden Systems nötig sind. Jedoch erfordert er, mehr noch als das ursprüngliche V-Modell, eine strikte Umsetzung der Entwicklungszyklen. Das könnte in der Praxis zu Problemen führen, da viele individuelle Faktoren und Umstände in der Realität in ein Projekt hineinspielen. Insbesondere ist es schwierig zu erwarten, dass sich kleine mittelständische Softwareunternehmen oder Unternehmen mit entsprechend geringen Ressourcen an gleiche Richtlinien halten können wie große etablierte Softwarehäuser.

3.2 An Integrated Approach to Safety and Security Based on System Theorie

Einen völlig anderen Ansatz präsentieren William Young und Nancy G. Leveson vom Massachusetts Institute of Technology, Cambridge in ihrem im Februar 2014 veröffentlichten Paper ¨An Integrated Approach to Safety and Security Based on Systems Theory." [10] Wie der Titel bereits verrät, wird hier versucht, die Safety & Security Frage mithilfe der Systemtheorie anzugehen und damit ein Modell zur Erfassung entsprechender Systeme zu entwerfen. Thematisch bewegen sich die beiden Autoren in einem weiten Spektrum von Systemen. Erwähnt werden beispielsweise Flugzeuge, Autos, Atomkraftwerke und medizinische Geräte, aber auch Systeme im Bereich der Raumfahrt, was nicht verwunderlich ist, bewegte sich Nancy G. Leveson doch lange Zeit im Bereich der NASA und ist heute Professorin für Aeronautics and Astronautics am oben genannten Institut. So verfolgt dieser Ansatz, im Gegensatz zum zuvor beschriebenen, eine weniger auf ein konkretes Problem, die Automobilindustrie, bezogen entwickelte, als eine allgemeingültige Lösung.

Idee Der Ansatz basiert auf der Idee, bereits vorhandene und erfolgreich eingesetzte Methoden für Safety-Analysen (STAMP + STPA), basierend auf systemtheoretischen Ansätzen, zu erweitern, um die notwendigen Security-Aspekte (STPA+SEC) miteinzubeziehen. Auf diese Methoden wird später eingegangen.

Um die grundsätzlichen Gedanken und Ideen hinter dem in diesem Paper beschriebenen Ansatz zu verstehen, zeigen Young und Leveson zunächst auf, was der Unterschied zwischen taktischer und strategischer Denkweise im Gebiet der Security ist, wobei der Lösungsansatz des Papers auf der strategischen basiert.

Die taktische Vorgehensweise unterscheidet sich essentiell von der strategischen, beginnend mit der grundlegenden Frage, wie die Schwachstellen eines Systems identifiziert und geschlossen werden können. Während in der taktischen die Schwachstellen gesucht werden ("Wo sind Schwachstellen?"), sucht die strategische die Elemente eines Systems, die beschützt werden müssen ("Was muss beschützt werden?").

Im weiteren taktischen Vorgehen werden die gefundenen Lücken geschlossen, wozu eine Priorisierung der Lücken notwendig ist. Daraus ergibt sich stets eine Verteidigung aus nachteiliger Position, da man auf Angriffe und neu aufgeflogene Lücken reagieren muss. Die taktische Vorgehensweise ist ein Bottom-Up Konzept.

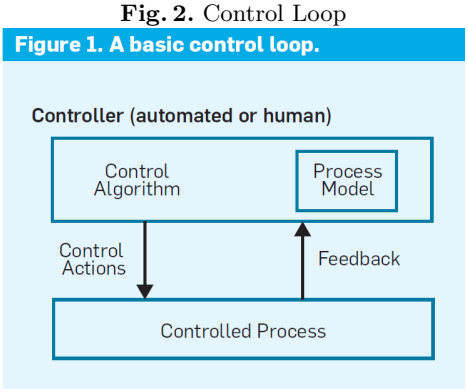
Im strategischen Top-Down Konzept wird im Gegensatz dazu nicht reaktionär gehandelt, sondern das System von Beginn an so konzeptioniert, dass die Anordnung der Komponenten hierarchisch strukturiert wird um zuvor identifizierte inakzeptable Verluste bereits architektonisch zu verhindern. Diese Strukturierung konkretisiert sich stufenweise, beginnend mit dem höchsten Abstraktionslevel. So entsteht ein Modell, das eine kleinere, besser kontrollierbare Menge an potentiellen Verlusten innehat und in dem Unvollständigkeiten einfach gefunden werden können.

Die bereits zuvor erwähnte Safety-Analysemethode STPA (Sytem-Theoretic Process Analysis) basiert auf einer Modellierung mithilfe der Methode STAMP (System-Theoretic Accident Model and Processses). STAMP erstellt Modelle für Systemkomponenten und deren gegenseitige Ursache und Wirkung. So werden zwischen jeder Stufe einer zuvor erstellten hierarchischen Kontrollstruktur sogenannte Control Loops eingebaut, die Prozesse kontrollieren, indem sie Control Action an diese senden und das anschließende Feedback auswerten (Fig. 2).

So werden sämtliche Komponenten stets kontrolliert, überwacht und auf Fehlverhalten untersucht. Der Controller des Prozesses kann hierbei automatisiert oder manuell konzipiert werden. Anschließend wird STPA angewandt, das sich aus den folgenden Schritten zusammensetzt. Zunächst werden die möglichen Fehlverhalten der Prozesse identifiziert, welche die zu schützenden Objekte gefährden könnten. Nun werden Control Actions identifiziert, die zu den Fehlverhalten der Prozesse führen können. Als letzter Schritt werden die Control Loops dahingehend untersucht, herauszufinden, in welchen Szenarien die zuvor identifizierten Control Actions enstehen können. Die Erweiterung von STPA um den Security-Anteil zu STPA-SEC wird umgesetzt, indem zum letzten ausgeführten Schritt

nicht nur Safety-Szenarien alleine, sondern zusätzlich mögliche Security-Szenarien, die eben diese Safety-Szenarien auslösen könnten, eingebaut werden.

Fig. 2. Control Loop



Quelle: William Young and Nancy G. Leveson: "An Integrated Approach to Safety and Security Based on Systems Theory" [10]

Eindruck Im Vergleich zum Lösungsansatz des Papers "Automotive Functional = Safety + Security"[4], scheint dieser auf der einen Seite abstrakter, allgemeiner und wenig konkret. Jedoch könnte man hoffen, dass sich dieser Ansatz, zumindest in Projekten mit entsprechend hoher Safety- und Security-Relevanz, besser realisieren lässt, da er nicht darauf basiert, einen bereits schwer umzusetzendes Modell (V-Modell) weiter aufzublähen und den Aufwand der einzelnen Entwicklungsstufen weiter zu erhöhen, sondern auf einem Analyseverfahren basiert, das nicht unmittelbar mit dem Entwicklungsprozess verdrahtet ist.

3.3 Resiliente Systeme

Um dem Eintreten gravierender unvorhersehbarer Fehlfunktionen durch bereits kleine Störungen in zu komplex gewordenen Systemen zu begegnen, wurde das Konzept der resilienten Systeme entwickelt, welche zusätzlich erwähnenswert sind. Dazu kann der Begriff Resilienz wie folgt definiert werden: "die Fähigkeit, tatsächlich oder potenziell widrige Ereignisse abzuwehren, sich darauf vorzubereiten, sie einzukalkulieren, sie zu verkraften, sich davon zu erholen und sich ihnen immer erfolgreicher anzupassen"[1]. Resilienz hat vor allem zum Ziel, Systeme widerstandsfähig zu machen, möglichst lange, auch unter Störungen, aufrechtzuerhalten und damit negative Auswirkungen abzuschwächen. Hierbei steht besonders die Lern- und Anpassungsfähigkeit von Systemen im Fokus [7]. Aufgrund der zusätzlichen Komplexität dieses Ansatzes wird in dieser Arbeit nicht detaillierter darauf eingegangen, ist für spätere Arbeiten aber sicher lohnenswert und spannend.

4 Konferenzen

Ein klares Signal zur steigenden Relevanz und Brisanz von Safety und Security ist die Zunahme der Konferenzen, die sich immer mehr mit diesen Themengebieten beschäftigen. Hier werden aktuelle Trends und möglicherweise kommende Entwicklungen betrachtet und diskutiert. Im Folgenden wird eine Auswahl von aktuellen relevanten Konferenzen mit deren Inhalt aufgeführt.

4.1 SafeComp

Die SafeComp ist eine dreitägige Konferenz, die 2015 in den Niederlanden stattfand und sich dem Gebiet "computer safety, reliability & security" annimmt.

Im vergangenen Jahr trug Cor Kalkman, Anästhesist am University Medical Center Utrecht (NL) einen Keynotespeak zum Thema Safety und Security mit dem Titel "Medical devices, Electronic Health Records and assuring Patient Safety: future Challenges?" vor. Hier wurde das Thema der medizinischen Geräte aufgegriffen, die durch zunehmende Vernetzung zum Ziel von Security-Angriffen werden und diese die Safety der Systeme beeinflussen könnten.

Ein weiterer Keynotespeak beschäftigte sich mit dem Thema der Sicherheit im Gebiet des Internet of Things, vorgetragen von Andrey Nikishin, Director im Kaspersky Lab in London mit dem Titel: "Does IoT stand for Internet of Threats and other stories?" Auch wenn der Titel generell scheint, hat das IoT eine große Bedeutung für die Entwicklung und Relevanz von Safety und Security. Auch im weiteren Verlauf der Konferenz waren die Themen stark von Safety und Security geprägt. So stand der erste Tag unter dem Motto "transport systems", wozu Vorträge wie "Flight Systems" und "automotive Systems" zählten. Am zweiten Tag war dies, wie bereits in einem der Keynotespeaks angerissenen, das Gebiet "medical systems" und am dritten "security & safety" mit den Vortragsthemen "Protection from security attacks" und "Cyber security and integration." [9]

4.2 ASQF Quality Day

Der ASQF Quality Day in Berlin beleuchtete im vergangen Jahr vor allem die Fragen, die sich an die Qualitätssicherung und an das Testen stellen, insbesondere in Hinblick auf IoT und Industrie 4.0. Der Keynotespeak der Leiterin des Fraunhofer FOKUS Berlin, Ina Schieferdecker handelte vom IoT-Testing, wohingegen sich andere Vorträge mit neuen Testkriterien, sowie der Testautomatisierung in vernetzten industriellen Systemen beschäftigten. So behandelte Dr. Jürgen Großmann, ebenfalls vom Fraunhofer FOKUS, in seinem Vortrag "Systematically combine security risk assessment and testing based on standards" eine mögliche Kombination von ISO 31000[14] und ISO 29119 [13] um Risikobewertung und Testen hinsichtlich der Cyber Security in immer stärker vernetzten Systemen zu verbinden. Auch Dipl.-Ing. Carsten J. Pinnow referierte mit dem Titel "Datensicherheit als erfolgskritisches Qualitätsmerkmal der Industrie 4.0" über die Relevanz von Security in industriellen Systemen.[3]

4.3 Chaos Communication Congress

Jährlich findet der Chaos Communication Congress, veranstaltet durch die weltweit agierende Hackercommunity Chaos Computer Club, in Hamburg statt. Hier werden viele Themen im Gebiet Security erörtert und diskutiert. Im vergangen Jahr (2015) trug beispielsweise Marie Moe, aus dem obigen Beispiel, die Ergebnisse ihre Nachforschungen an ihrem eigenen Herzschrittmacher vor und zeigt damit mögliche durch Security-Attacken ausgelöste Safety-Risiken. Alle Vorträge sind online auch im Nachhinein als Videostream frei zugänglich.[5]

5 Ausblick

In Zeiten stetig wachsender vernetzter und dadurch an Komplexität gewinnender Systeme, wird die Relevanz der Thematik Sicherheit in der Kombination Safety und Security stetig wachsen. Die Ausbreitungen im Bereich des Internet of Things in all seinen Facetten, sowie die Digitalisierung der Industrie (Stichwort Industrie 4.0) machen klar, dass es sich nicht nur um einen aktuellen Trend, sondern um eine anhaltende Entwicklung handelt. Auch wird es nicht bei den bisher erwähnten und auf Konferenzen immer häufiger diskutierten betroffenen Bereichen wie medizinischen Geräten, dem Verkehr, ob in der Luft (Flugzeuge, Drohnen) oder auf der Straße oder sensiblen Einrichtungen wie Kraftwerken etc. bleiben. Vielmehr werden sich immer mehr Bereiche, die selbst noch in einem eher frühen Entwicklungsstadium stecken, etwa wie die Robotik, die Mensch-Computer-Interaktion und die künstliche Intelligenz, mit dieser Problematik beschäftigen müssen.

Um dafür zu arbeiten, dass allerlei solcher Systeme sicher werden oder sicher bleiben, müssen neue Methoden entwickelt, geprüft und getestet werden, die solche Systeme erfassen und analysieren können. Nur so kann es gelingen, passende und sichere Systeme zu entwickeln. Auch die Qualitätssicherung und das Testen solcher Systeme wird eine sehr große Rolle spielen. Hier muss die Forschung vorangetrieben werden, um neue Verfahren zum Entwurf von Tests, automatisiert oder manuell, welche die Aspekte beider Bereiche, Safety und Security, gleichermaßen berücksichtigen und idealerweise kombinieren, zu entwickeln. Denkbar wären beispielsweise weiterentwickelte automatisierte Angriffssimulationen und Sicherheitstests, die durch das Nutzen von Security-Lücken Fehlfunktionen im Safety-Bereich auslösen. Auch mögliche Kombinationen von Teilsystemen und die daraus resultierende wachsende Komplexität sind durch die Testverfahren abzudecken. Hierzu müssen sich Expertengruppen aller Komponenten des Systems zusammensetzen, sich austauschen, diskutieren und entwickeln, um eine lückenlose Testkette des Gesamtsystems zu ermöglichen. [7]

References

1. acatech: Resilience-by-Design: Strategie für die technologischen Zukunftsthemen (2014)
2. ADAC: https://www.adac.de/infotestrat/technik-und-zubehoer/fahrerassistenzsysteme/sicherheitsluecken/sicherheitsluecken.aspx?ComponentId=224182SourcePageId=8749quer=sicherheitsluecken (eingesehen am 09.03.2016)
3. ASQF: https://www.asqf.de/fachgruppentermine-anzeige/events/id-09122015-software-quality-day-2015-fraunhofer.html (eingesehen am 28.02.2016)
4. Burton, Simon, Likkei, Jürgen, Wolf, Marko: Automotive Functional = Safety + Security (2012)
5. Chaos Communication Congress: https://events.ccc.de/ (eingesehen am 28.02.2016)
6. Kornecki, Andrew J., Zalewsk, Janusz: Safety and Security in Industrial Control (2010)
7. Menz, Nadja, Hoepner, Petra, Tiemann, Jens, Koußen, Frank: Safety and Security in Industrial Control (2010)
8. Moe, Marie, Leverett, Eireann: Unpatchable: Living with a vulnerable implanted device (2015)
9. safecomp: http://safecomp2015.tudelft.nl/ (eingesehen am 28.02.2016)
10. Young, William, Leveson, Nancy G.: An Integrated Approach to Safety and Security Based on Systems Theory (2014)
11. ISO 14508: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39779 (eingesehen am 28.02.2016)
12. ISO 26262: http://www.iso.org/iso/catalogue_detail?csnumber=43464 (eingesehen am 28.02.2016)
13. ISO 29119: http://www.iso.org/iso/catalogue_detail.htm?csnumber=45142 (eingesehen am 28.02.2016)
14. ISO 31000: http://www.iso.org/iso/home/standards/iso31000.htm (eingesehen am 28.02.2016)