Elektrotechnik & Informationstechnik (2021) 138/7: 449–453. https://doi.org/10.1007/s00502-021-00930-0



# Safety und Security – ein Spannungsfeld in der industriellen Praxis

S. Hollerer, W. Kastner, T. Sauter

Die Grenzen zwischen Informationstechnologie (IT) und Betriebstechnik (OT) verschwimmen zunehmend, wodurch die Schutzziele Informations- und Datensicherheit (Security) und Betriebssicherheit (Safety) ebenfalls immer stärker voneinander abhängen. Beispielsweise können Cyber-Angriffe Safety-Funktionen verändern und dadurch Menschen und die Umgebung gefährden. Umgekehrt kann der Missbrauch einer Safety-Funktion zum Stopp einer Maschine oder Produktionslinie führen und so die Verfügbarkeit beeinträchtigen. Der vorliegende Beitrag beschäftigt sich damit, wie verschiedene österreichische Stakeholder der Industrie aktuell mit Security- und Safety-Risiken umgehen, um unerwünschte Situationen zu vermeiden oder zu verhindern. Bei dieser Analyse werden sowohl Hersteller von Produkten oder Komponenten als auch Integratoren und Betreiber industrieller Systeme befragt. Es werden dabei die Themengebiete sichere Infrastrukturen und Systemarchitekturen sowie Risikomanagement betrachtet. Die daraus abgeleiteten Ergebnisse bieten Einblicke in den aktuellen Stand beim Umgang mit Safety und Security in der Industrie.

Schlüsselwörter: Security; Safety; IT/OT-Konvergenz; Industrie 4.0

***Safety and security – a field of tension in industrial practice.***

*The borders between Information Technology (IT) and Operational Technology (OT) become indistinct, leading to an increasing interdependence between the protection goals of security and safety. For example, a cyber attack that alters safety functions may in turn lead to threats to people and the environment. Conversely, the misuse of safety functions may cause a machine or production line to stop working, which impacts availability. This article identifies how Austrian stakeholders of industrial automation handle security and safety risks to avoid or prevent undesired situations. The stakeholder analysis performed takes vendors of products or components, integrators, and operators of industrial architectures into account. Subject areas of this study include secure infrastructures, system architectures, and risk management. The results obtained provide insights into the current practices with regard to safety and security in the industry.*

*Keywords: security; safety; IT/OT convergence; Industry 4.0*

Eingegangen am 9. Juli 2021, angenommen am 6. September 2021, online publiziert am 17. September 2021


## 1. Einleitung und Problemstellung

Getrieben durch aktuelle Trends im Kontext von Industrie 4.0 konvergieren in der industriellen Automatisierung die beiden Domänen Informationstechnologie (IT) und Betriebstechnik (OT) immer stärker, wodurch die vormals klaren Grenzen der beiden Domänen zunehmend verschwimmen. Zur IT zählt man Anwendungen der Unternehmensführung, Informations- und Kommunikationstechnologie im betrieblichen Umfeld (IKT) und Software zur Bearbeitung und Verteilung von Daten der Produktionsanlagen. Die OT hingegen umfasst Hardware, industrielle Kommunikationssysteme und Software-Komponenten zur Überwachung und Kontrolle technischer Prozesse von Maschinen. Die IT beschäftigt sich primär mit IT-Sicherheit (Security), um sich vor Cyber-Angriffen durch zur Gewährleistung von Vertraulichkeit, Integrität und Verfügbarkeit zu schützen. Die OT hat als oberstes Schutzziel die funktionale Sicherheit (Safety) zu gewährleisten, um sowohl das Umfeld als auch Menschen vor unerwünschten Operationen zu schützen, die beispielsweise Bediener von Maschinen verletzen könnten [1, 2].

Durch die zunehmende Verschmelzung der beiden Domänen IT und OT können Cyber-Angriffe Auswirkungen auf die funktionale Sicherheit haben. Beispielsweise können Angreifer durch die Ausnutzung von IT-Schwachstellen ein Safety Instrumented System (SIS) manipulieren. Das korrumpierte SIS wird daraufhin nicht bei Bedarf oder im falschen Moment aktiviert, womit in weiterer Folge Verletzungen an Personen (z.B. während der Bedienung der Maschine) nicht ausgeschlossen oder Schäden an der Produktionsanlage nicht mehr abgewehrt werden können. Außerdem ist es möglich, die Safety-Funktion absichtlich auszulösen, wodurch die Maschine oder Produktionslinie den Betrieb einstellt, was sich negativ auf die Verfügbarkeit auswirkt [3] und wirtschaftlichen Schaden verursacht. Neben einem direkten Angriff auf die Safety-Funktion können Cyber-Angriffe gegen Benutzerschnittstellen (beispielsweise Web-Applikationen) ebenfalls die Safety in weiterer Folge negativ beeinflussen [4–6].

Die genannten Beispiele unterstreichen die Notwendigkeit, Safety und Security gesamtheitlich zu betrachten. Dazu wurde das TÜV AUSTRIA #SafeSecLab Research Lab for Safety and Security in Industry, eine Kooperation zwischen der TU Wien und TÜV AUSTRIA, ins Leben gerufen. Es beschäftigt sich mit einer holistischen Betrachtung von Safety und Security auf unterschiedlichen Ebenen. Neun

Diese Arbeit wurde ermöglicht durch das TÜV AUSTRIA #safeseclab Research Lab for Safety and Security in Industry, eine Forschungskooperation zwischen der TU Wien und TÜV AUSTRIA.

**Hollerer, Siegfried,** TU Wien, Treitlstr. 1-3/4. Stock/E191-03, 1040 Wien, Österreich (E-Mail: siegfried.hollerer@tuwien.ac.at); **Kastner, Wolfgang,** TU Wien, Wien, Österreich; **Sauter, Thilo,** TU Wien, Wien, Österreich

vernetzte Einzelprojekte analysieren das Zusammenspiel und die gegenseitige Abhängigkeit der beiden Schutzziele auf Komponenten-Ebene bis hinauf zur Gesamtarchitektur im Kontext der industriellen Automatisierung inklusive eines dafür entwickelten Bedrohungsmodells und davon abgeleiteten Risikomanagements. Ziel der Projekte ist es, Verfahren sowie technische und organisatorische Maßnahmen zu identifizieren, die Safety und Security industrieller Komponenten, Systeme und Anlagen entlang ihres gesamten Lebenszyklus gewährleisten.

Der vorliegende Beitrag ist Teil des Bedrohungsmodells [1] und beschäftigt sich damit, wie verschiedene Interessengruppen der industriellen Automatisierung (im weiteren Verlauf als "Stakeholder" bezeichnet) aktuell mit Safety- und Security-Risiken umgehen. Dazu wird in Abschn. 2 die gewählte Methodik zur Stakeholder Analyse erläutert und anschließend in Abschn. 3 die davon erhaltenen Ergebnisse diskutiert. Abschließend gibt Abschn. 4 Ausblicke auf weitere Vorhaben, die auf der präsentierten Analyse aufbauen.

## 2. Methodik

Im Rahmen einer Stakeholder-Analyse wurden sechs Unternehmen eingeladen, aktuelle und mögliche künftige Herausforderungen in den Bereichen Safety und Security sowie deren gesamtheitliche Sichtweise durch die IT/OT Konvergenz zu identifizieren. Ein Unternehmen im Bereich Energie und Gebäudetechnik stellt sowohl Produkte oder Komponenten her, integriert diese zu Automatisierungssystemen und betreibt selbst Automatisierungssysteme. Ein weiterer Stakeholder ist Integrator und Betreiber im öffentlichen Transport. Zwei Hersteller von Produkten und Komponenten nahmen an der Analyse teil, die in den Sektoren Kraftfahrzeugtechnik respektive Automatisierungstechnik platziert sind. Zwei Betreiber aus dem Bereichen Logistik bzw. Verfahrenstechnik stellten Informationen aus diesem Blickwinkel bereit.

Die Unternehmen nahmen dazu an einer Onlinebefragung teil. Der verwendete Fragebogen umfasste 70 Fragen, die sowohl technische als auch organisatorische Aspekte im Rahmen von Industrie 4.0 beleuchteten, wie z.B. verwendete Infrastrukturen, Systemarchitekturen und Kommunikation innerhalb des Gesamtsystems, sowie Safety, Security und Bedrohungs- bzw. Risikomanagement hinterfragten. Abbildung 1 illustriert die Struktur und die dazu gehörigen Themengebiete des Fragenkatalogs.

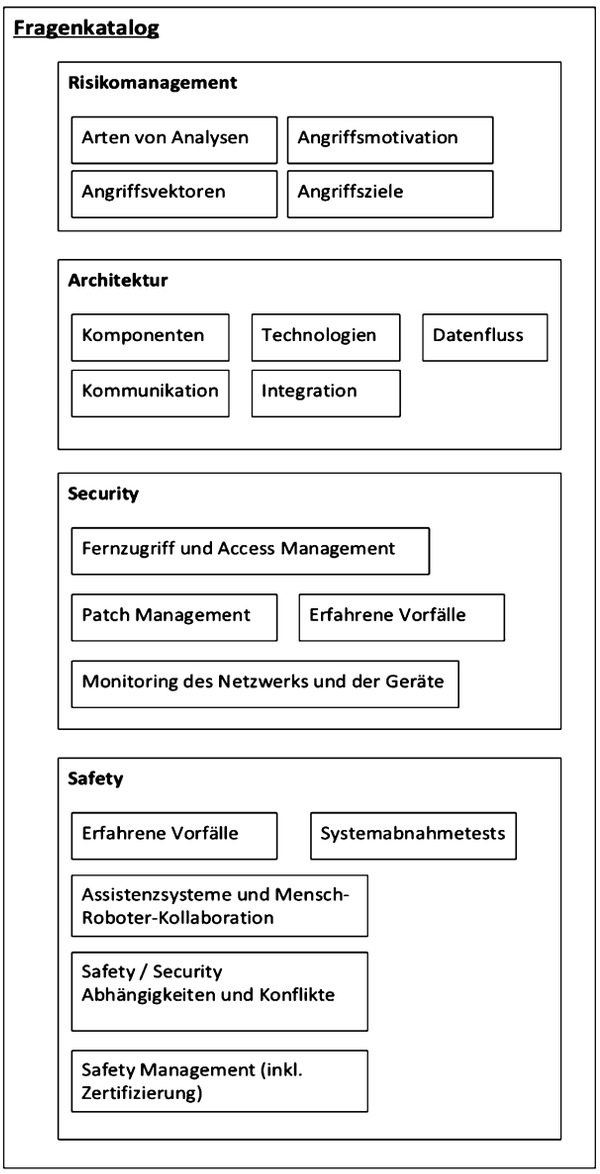


**Abb. 1. Themengebiete der Stakeholder Analyse**

Die Kategorie *Bedrohungs- bzw. Risikomanagement* befasst sich damit, welche Arten von Analysen durchgeführt und welcher Kontext dafür gewählt wurde. Beispielsweise wurde nach Compliance-Anforderungen oder der Erfassung externer Parteien im Risikomanagement gefragt, um Risiken, die ihren Ursprung nicht im System des Teilnehmers haben, dennoch identifizieren zu können.

Fragen über den *Aufbau der Architektur* geben Aufschluss über verwendete Referenzarchitekturmodelle und Technologien, um das konkrete Automatisierungssystem des Teilnehmers grob zu erkennen. Zusätzlich erlauben diese Fragen Rückschlüsse darauf, wie Systemkomponenten in Betrieb gehalten werden, wie einzelne Komponenten erfasst werden bzw. wie mit Alt-Systemen (Legacy Systems) umgegangen wird.

Die Fragenkategorie *Kommunikation innerhalb des Gesamtsystems* hat zum Inhalt, welche (industriellen) Kommunikationssysteme (z.B. Industrial Ethernet, Feldbusse), IKT-Protokolle (z.B. MQTT, HTTP) in Verwendung sind. Des weiteren werden Echtzeit-Anforderungen, Fernwartungszugänge und Konfigurationsänderungen des Netzwerkes und die Meinung zu OPC UA (TSN) als Weg zur Vereinheitlichung hinterfragt.

Die Rubrik *Security* befasst sich mit vorhandenen technischen und organisatorischen Sicherheitsmaßnahmen. Zusätzlich wurde nach Cyber-Sicherheitsvorfällen und deren Zusammenhang mit Safety gefragt, um die gegenseitige Abhängigkeit von Security und Safety aus dieser Sicht ebenfalls zu erfassen.

Die Fragegruppe *Safety* befasst sich mit eventuellen vergangenen Sicherheitsvorfällen und deren möglichem Zusammenhang mit Cyber-Security. Weitere Themen sind Mensch-Roboter-Kollaboration (MRK), Systemabnahmetests sowie Informationen über aktuell im Einsatz befindliche Safety-Controller.

Generell zielten die Fragen darauf ab, mögliche Einflüsse von Schwachstellen, Angriffsvektoren, zugehörigen Angreiferarten und bereits vorhandenen Gegenmaßnahmen auf die zugrunde liegenden System- und Netzwerkarchitekturen zu identifizieren. Die Durchführung der Befragung erfolgte online durch das Umfragetool LimeSurvey.[1]

[1] https://www.limesurvey.org/de/.

**Tab. 1. Ausschnitt der Ergebnisse der Stakeholder Analyse**

| Kategorie | Ergebnis |
|---|---|
| Risikomanagement | Die Risiko-/Bedrohungsanalyse findet nicht einheitlich statt. |
| Risikomanagement | Bei 89 % sind geschäftskritische Systeme in der OT. |
| Risikomanagement | 33 % betrachtet Lieferkette nicht im Risikomanagement. |
| Risikomanagement | Durchführung von Sicherheitsüberprüfungen unterschiedlich: 44 % führen technische und organisatorische Sicherheitsüberprüfungen durch. |
| Architektur | 89 % trennt IT und OT in unterschiedliche Netze. |
| Architektur | Bei 89 % erfolgen Fernzugriffe über abgesicherte Bereiche im Netzwerk. |
| Architektur | 78 % der Befragten ist der Begriff RAMI 4.0 unbekannt. |
| Architektur | 89 % planen Änderungen an der implementierten Architektur. |
| Architektur | 89 % verwenden drahtgebundene Feldbussysteme parallel zu Ethernet. |
| Architektur | Profbus (78 %), Profinet (67 %), MQTT (67 %) sind häufig in Verwendung. |
| Architektur | Zwischen IT und OT sind oft HTTPS (100 %), HTTP (78 %) und SSH (78 %) im Einsatz. |
| Security | Security-Anforderungen werden unterschiedlich wahrgenommen. |
| Security | 89 % gehen aktiv gegen Social Engineering vor. |
| Security | Alle führen Backups durch, 78 % überprüfen diese. |
| Security | 25 % alarmieren bei auffälligem Verhalten nicht automatisch. |
| Security | 12 % loggt die Netzwerkkommunikation und Systemzugriffe nicht mit. |
| Security | 78 % wurden Opfer eines Cyber-Sicherheitsvorfalls. |
| Safety | Bei 67 % der Safety-relevanten Vorfälle war Cyber-Security involviert. |
| Safety | Redundanz (78 %) und hohe Verfügbarkeit (67 %) sind die wichtigsten Safety-relevanten Anforderungen. |
| Safety | Zykluszeit ist die einzige Echtzeit-Anforderung. |
| Safety | 78 % führten bereits Systemabnahmetests und eine Risikoanalyse betreffend Safety und Security durch. |
| Safety | Abhängigkeiten zwischen Safety und Security sind durch ACLs, IP-based Whitelisting, Reverse-Proxies und die regelmäßige Aktualisierung externer Schnittstellen adressierbar. |

## 3. Ergebnisse und Diskussion

Tabelle 1 fasst die Auswertung der Analyse-Ergebnisse kurz zusammen.

**Risikomanagement** Alle befragten Unternehmen führen grundsätzlich Risiko- bzw. Bedrohungsanalysen durch. Die Durchführung und der Gegenstand (Scope) der Analyse unterscheiden sich jedoch stark voneinander. Der Scope der Risiko- bzw. Bedrohungsanalysen reicht von einer domänenspezifischen (z.B. durchgeführt durch OT Security HAZOP) bis hin zu einer organisationsübegreifenden, klassischen Risikoanalyse (z.B. mittels Global Corporate Risk Assessment). Neben der häufig verschiedenen Detailtiefe der Analysen sind auch Unterschiede in der Themenbreite erkennbar. Beispielsweise befassen sich "IT- Sicherheitsaudits" ausschließlich mit Security-Aspekten der Architektur, während sich "OT Security HAZOP" sowohl den Schutzzielen Security als auch Safety widmen.

Fast alle befragten Teilnehmer haben geschäftskritische Systeme in ihrer industriellen Architektur verankert, die permanent in Betrieb gehalten werden müssen. Bei einem Drittel ist im Risikomanagement die Lieferkette (Supply Chain) nicht berücksichtigt. Dadurch sind auf die Lieferkette zurückgehende Risiken für diese Gruppe nicht identifizierbar.

Die Durchführung von Sicherheitsüberprüfungen erweist sich als unterschiedlich stark ausgeprägt. Unter den Aspekt der technischen Sicherheitsüberprüfungen fallen u.a. Penetration Tests und Prozesse, die dazu dienen, eine Angriffsmöglichkeit zu eliminieren, indem Schwachstellen gepatcht und nicht benötigte Dienste abgeschaltet werden (Hardening). Organisatorische Sicherheitsüberprüfungen beinhalten beispielsweise Prüfungen nach den internationalen Standards betreffend IT-Security (ISO 27001) oder betreffend OT-Security (IEC 62443), die einen ganzheitlichen organisatorischen sowie technischen Ansatz der Absicherung von IT- und OT-Systemen verfolgen. 44 % führen sowohl technische als auch organisatorische Sicherheitsüberprüfungen durch, während 22 % ausschließlich technische und 11 % ausschließlich organisatorische Sicherheitsüberprüfungen durchführen. Um alle Risiken identifizieren zu können, ist die Durchführung beider Arten von Sicherheitsüberprüfungen notwendig.

**Architektur** Der überwiegende Teil der Befragten trennt die Domänen IT und OT in unterschiedliche Netze auf. In Einzelfällen sind aber auch Architekturen vorzufinden, die weder über eine physische noch eine logische Netzwerk-Segmentierung verfügen. Fernzugriffe erfolgen zumeist über abgesicherte Bereiche im Netzwerk. Unter abgesicherten Bereichen werden demilitarisierte Zonen (DMZ) oder Jump Hosts verstanden. Generell orientieren sich die Systemarchitekturen (wenig überraschend) an historisch gewachsenen Systemen bzw. an den konkreten Notwendigkeiten des jeweiligen Unternehmens. Abstraktere, umfassende Ansätze wie z.B. das Referenzarchitekturmodell Industrie 4.0 (RAMI 4.0) [7], das Funktionen, Daten und Kommunikation von der Komponenten- bis zur Geschäftsebene untergliedert und außerdem auch den Lebenszyklus der einzelnen Elemente berücksichtigt [8], besitzen in der Praxis scheinbar noch keine Bedeutung. Nur 11 % der Befragten kennen den Begriff RAMI 4.0, im Unternehmen verankert ist er jedoch nicht.

Interessant ist, dass fast alle Teilnehmer Änderungen an ihrer Systemarchitektur planen, mit gewünschter Bereinigung von historisch gewachsenen Lösungen. 67 % planen zusätzlich die Integration eines neuen Systems, während 45 % Änderungen bei Dienstleistungs-Güte-Vereinbarungen (Service Level Agreements, SLAs) oder Aktualisierung bzw. Austausch von nicht mehr von Herstellern unterstützten Systemen (Legacy Systemen) ins Auge fassen.

Bei den im Einsatz befindlichen Kommunikationssystemen zeigt sich die ganze Vielfalt der historischen Entwicklung. Der Großteil der Stakeholder hat parallel Ethernet (auch Echtzeit-Ethernet) und

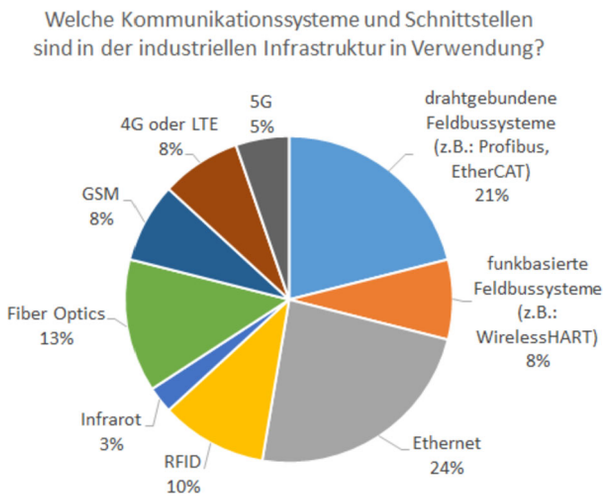


**Abb. 2. Verwendete Kommunikationsprotokolle**

drahtgebundene Feldbusse in Verwendung, wie in Abb. 2 zu erkennen ist. Funkbasierte Lösungen (z.B. WirelessHART) und zelluläre Funknetze (z.B. GSM, 4G / LTE, 5G) sind vergleichsweise selten im Einsatz.

Bei den verwendeten Übertragungsprotokollen im OT-Bereich dominieren Profibus (78 %), Profinet (67 %) und MQTT (67 %). HART (22 %), CAN (33 %), EtherCAT (44 %) und legacy OPC (33 %) sind dagegen bei den befragten Teilnehmern deutlich seltener in Verwendung. Überraschenderweise ist OPC UA bei 67 % der Befragten bereits im Einsatz. Für die Kommunikation zwischen IT und OT ist bei jedem Teilnehmer HTTPS in Verwendung. Das unverschlüsselte Pendant HTTP ist mit 78 % allerdings nach wie vor weit verbreitet. Die Kommunikationsprotokolle SSH (78 %), SMB (67 %) und VNC (56 %) kommen beim Großteil der Befragten vor, am unteren Ende der Liste liegen Siemens S7 und SNMP mit jeweils 45 %.

Ausschreibungen beim Geräteeinkauf umfassen unterschiedliche Security-Anforderungen. Die häufigsten Anforderungen sind die Möglichkeit, ein Berechtigungskonzept abzubilden (67 %), und die Implementierung einer Anmeldung, um den Zugriff auf das Gerät (56 %) einschränken zu können. 33 % fordern die Möglichkeit der Verschlüsselung der Kommunikationsprotokolle. Der Verzicht auf die Verwendung von unsicheren Legacy Protokollen (z.B. SNMPv1, SSHv1) ist nur für 11 % der Befragten eine Anforderung. Außerdem ging aus der Auswertung der Antworten dieser Frage hervor, dass nicht allen Herstellern Security-spezifische Anforderungen der Integratoren bekannt sind.

**Security** Nahezu alle befragten Teilnehmer führen regelmäßig Security Awareness Trainings für ihre Mitarbeiter durch, um gegen Social Engineering gewappnet zu sein. Bei Social Engineering [9] wird versucht, eine Person zu manipulieren, um sich Zugang zum System zu verschaffen. Die Security Awareness Trainings helfen den Mitarbeitern selbständig Social Engineering Angriffe zu erkennen. Neben dieser Maßnahme werden zusätzlich Phishing-Kampagnen durchgeführt, um einen erhöhten Schutz gegen diesen Angriffsvektor zu erzielen.

Ausnahmslos alle Befragten gaben an, regelmäßig Backups von sensiblen Daten durchzuführen. 23 % überprüfen diese jedoch nicht, wodurch im Bedarfsfall der Schutz gegen Datenverlust für diese Gruppe dennoch ausbleiben kann.

25 % der befragten Stakeholder verfügen über keine Mechanismen, die bei einem auffälligen Verhalten einen Alarm erzeugen (z.B. Intrusion Detection Systems). Demnach sind für diese Architekturen verdächtige Aktivitäten nur manuell erkennbar, wodurch die Erkennungsrate deutlich geringer ist. Eine geringe Anzahl der Befragten zeichnet die Netzwerkkommunikation nicht auf und loggt auch Systemzugriffe nicht. Dadurch wird eine frühzeitige Erkennung erschwert, ob das System einem Cyber-Angriff oder Infektion ausgesetzt ist.

Durchaus überraschend war, dass mehr als Dreiviertel der befragten Stakeholder angaben, in der Vergangenheit bereits Opfer von mindestens einem Cyber-Sicherheitsvorfall geworden zu sein.

**Safety** 33 % der Stakeholder hatten in der Vergangenheit mindestens eines Sicherheitsvorfall, der die funktionale Sicherheit betraf. Davon hatten 67 % der Sicherheitsvorfälle mit Cyber-Security zu tun. Aus diesen Ergebnis geht eine direkte Abhängigkeit zwischen Safety und Security hervor.

Bei den zu erfüllenden Safety-Anforderungen gaben 78 % der Teilnehmer Redundanz und 67 % hohe Verfügbarkeit an. 56 % müssen geringe Fehlertoleranzzeit und die Erreichung eines sicheren Zustands (Safe State) gewährleisten können. Die Rückwirkungsfreiheit (Freedom from Interference) ist für 45 % der Befragten wichtig. 78 % der Teilnehmer gaben ausschließlich die Zykluszeit von Steuerungen als zu erfüllende Echtzeit-Anforderung an. Die restlichen 22 % müssen keine Echtzeit-Anforderungen erfüllen.

78 % der Stakeholder führten bereits Systemabnahmetests und eine Risikoanalyse der Anwendungen ihrer Systeme betreffend Safety und Security durch. Der übrige Teil plant dies künftig anzubieten oder durchzuführen. Dieses Thema wird demnach von allen Stakeholdern als wichtig empfunden und entsprechend adressiert.

Auf der einen Seite erfordert Security häufige Updates, die identifizierte Security-Schwachstellen behebt, auf der anderen Seite erfordert die Safety-Zertifizierung, keine Änderungen am System durchzuführen. Ein Stakeholder geht mit diesem Konflikt um, indem externe Schnittstellen regelmäßig aktualisiert werden und nur die Safety-relevanten Kernfunktionen der OT Komponente zertifiziert werden. Außerdem sind zentrale Reverse-Proxies zwischen den Schnittstellen und Applikationen in Verwendung, die separat aktualisiert werden und so eine zusätzliche Security-Schicht bieten. Des Weiteren sind Access Control Lists (ACLs) und IP-based Whitelisting in Verwendung, um die Security zu erhöhen, während die Safety-Funktion für autorisierte Personen uneingeschränkt erreichbar bleibt.

## 4. Zusammenfassung

Die vorgestellte Analyse gab Einblicke in den aktuellen Umgang mit Safety und Security in der österreichischen Industrie bei ausgewählten Stakeholdern. Aus den Ergebnissen geht beispielsweise hervor, dass für die Risiko- bzw. Bedrohungsanalyse sowohl verschiedene Methodiken gewählt, als auch unterschiedliche Aspekte abgedeckt werden. Dadurch erhöht sich die Wahrscheinlichkeit unterschiedlicher Auffassungen von denselben Risiken und der Effektivität der implementierten Schutzmechanismen. Das Referenzarchitekturmodell RAMI 4.0 [7], das sowohl Safety und Security in industriellen Architekturen berücksichtigen ließe, hat einen geringen Bekanntheitsgrad und wird in der Industrie aktuell noch nicht eingesetzt.

Auffallend ist, dass industrielle Architekturen und Komponenten attraktive Cyber-Angriffsziele geworden sind, da dreiviertel der Befragten bereits Opfer eines Cyber-Sicherheitsvorfalls wurden. Die starke gegenseitige Abhängigkeit der beiden Schutzziele Safety und Security wurde untermauert, da der Großteil der von den Teilnehmern erfahrenen Safety-relevanten Vorfälle mit Cyber-Security zusammen hing. Darüber hinaus zeigte sich, dass aus der klassischen

IT bekannte Vorgehensweisen, wie Continuous Integration oder Angriffserkennung mit Security Information and Event Management (SIEM) Systemen derzeit noch nicht in der OT-Domäne angekommen sind. Diese Systeme kombinieren die beiden Konzepte Security Information Management (SIM) und Security Event Management (SEM) für die Echtzeitanalyse von Sicherheitsalarmen.

Aufbauend auf den Ergebnissen werden in weiteren Schritten gemeinsam mit den Stakeholdern Szenarien für künftige Systemarchitekturen ausgearbeitet und entwickelt, die spezifische industrielle Anforderungen für Safety und Security während des Lebenszyklus eines industriellen Automatisierungssystems aufzeigen sollen. Auf dieser Basis werden Design- und Implementierungs-Beispiele in der TU Wien Pilotfabrik abgeleitet, die als Proof of Concept für die Umsetzung von Anwendungsfällen dienen.

In jedem Fall verdeutlichen die Ergebnisse der Befragung die Notwendigkeit eines einheitlichen, ganzheitlichen Ansatzes, um Risiken betreffend Security und Safety vollumfänglich erkennen und bewerten zu können. Gleichzeitig stellt die Analyse Informationen zur Verfügung, die bei der Erstellung dieser Methodologie mitberücksichtigt werden können. Es wird bereits an einem entsprechenden Ansatz gearbeitet, der neben der Identifizierung der Risiken und deren Abhängigkeiten adäquate technische und organisatorische Schutzmechanismen und Gegenmaßnahmen bereitstellen soll. Das TÜV AUSTRIA #SafeSecLab Research Lab for Safety and Security in Industry von TU Wien und TÜV AUSTRIA hat es sich dabei zum Ziel gesetzt, zukunftsgerichtete Leistungen und Verfahren zu entwickeln, die zu einer integrierten Absicherung von OT aus der Perspektive "Security for Safety" beitragen.

**Funding Note** Open access funding provided by TU Wien (TUW).





**Literatur**

1. Hollerer, S., Kastner, W., Sauter, T. (2021): Towards a threat modeling approach addressing security and safety in OT environments. In 17th IEEE international conference on factory communication systems (WFCS). 4 pp.
2. Novak, T., Treytl, A., Palensky, P. (2007): Common approach to functional safety and system security in building automation and control systems. In 2007 IEEE conference on emerging technologies and factory automation (EFTA).
3. Di Pinto, A., Dragoni, Y., Carcano, A. (2018): TRITON: the first ICS cyber attack on safety instrument systems – understanding the malware, its communications and its OT payload. Black Hat USA
4. Wolf, M., Serpanos, D. (2018): Safety and security in cyber-physical systems and Internet-of-things systems. Proc. IEEE. https://doi.org/10.1109/JPROC.2017.2781198
5. Hollerer, S., Fischer, C., Brenner, B., Papa, M., Schlund, S., Kastner, W., Fabini, J., Zseby, T. (2021): Cobot attack: a security assessment exemplified by a specific collaborative robot. In 10th CIRP sponsored conference on digital enterprise technologies.
6. Grau, A., Indri, M., Bello, L., Sauter, T. (2021): Robots in industry: the past, present, and future of a growing collaboration with humans. IEEE Ind. Electron. Mag. https://doi.org/10.1109/MIE.2020.3008136.
7. Heidel, R., Hoffmeister, M., Hankel, M., Döbrich, U. (2019): Industrie 4.0 – the reference architecture model RAMI 4.0 and the Industrie 4.0 component. VDE Verlag, 150 pp.
8. Jasperneite, J., Sauter, T., Wollschlaeger, M. (2020): Why we need automation models: handling complexity in Industry 4.0 and the Internet of things. IEEE Ind. Electron. Mag. https://doi.org/10.1109/MIE.2019.2947119.
9. Bodungen, C., Singer, B., Shbeeb, A., Wilhoit, K., Hilt, S. (2016): Hacking exposed industrial control systems: ICS and SCADA security secrets & solutions. McGraw-Hill Education.

## Autoren

**Siegfried Hollerer**
arbeitete nach Abschluss seines Master-Studiums mehrere Jahre als Penetration Tester, führte Überprüfungen von Web-Applikationen, System Hardening Checks und Social Engineering durch und erwarb das Zertifikat OSCP (Offensive Security Certified Professional). Darüber hinaus führt Siegfried Risiko-Assessments auf Basis der Normenreihe IEC 62443 durch, die sich mit industrieller Security befasst.

**Wolfgang Kastner**
leitet den Forschungsbereich Automatisierungssysteme an der TU Wien. Zu seinen Forschungsinteressen zählen Entwurf, Analyse und Modellierung verteilter Automatisierungssysteme und ihre nahtlose Integration in das Internet der Dinge im industriellen Umfeld (IIoT) unter besonderer Berücksichtigung von Wissensrepräsentation sowie Sicherheitsaspekten.

**Thilo Sauter**
ist Professor am Institut für Computertechnik der TU Wien. Zudem war er Gründungsdirektor des Departments für Integrierte Sensorsysteme an der Donau-Universität Krems in Wiener Neustadt. Seine Interessen umfassen intelligente Sensoren und industrielle Kommunikationssysteme mit dem Schwerpunkt auf Echtzeit-, Sicherheits- und Integrationsfragen. Thilo Sauter ist IEEE Fellow.