Elektrotechnik & Informationstechnik (2021) 138/7: 447–448. https://doi.org/10.1007/s00502-021-00944-8

Safety und Security

W. Kastner, T. Sauter

angenommen am 21. September 2021, online publiziert am 1. Oktober 2021

Ao.Univ.Prof. Dipl.-Ing. Dr.techn.
Wolfgang Kastner

Ao.Univ.Prof. Dipl.-Ing. Dr.techn.
Thilo Sauter

Sicherheit ist für viele Bereiche im industriellen Umfeld ein zentrales Thema. Dahinter verbergen sich genau genommen zwei Themenfelder, die im Englischen durch die Begriffe *Safety* und *Security* unterschieden werden. Safety bezeichnet funktionale Sicherheit und Schutz, Security dagegen Informations- und Datensicherheit. Während Safety die Minimierung von Gefahren oder das Ausbleiben katastrophaler Folgen für Benutzer/innen und deren Umgebung zum Ziel hat, soll Security verhindern, dass Angreifer/innen unbefugt Ressourcen nützen können. Aus historischer Sicht sind diese beiden Felder mit ihren eigenen Disziplinen und Methoden unterschiedlich gewachsen. Maßnahmen und Vorschriften im Bereich der Safety existieren seit dem ausgehenden 19. Jahrhundert, während Security erst durch das Aufkommen der IT relevant wurde.

Speziell im industriellen Kontext wurden beide Aspekte der Sicherheit bis in die jüngste Zeit getrennt betrachtet. Die heute stark miteinander verbundenen Systeme, gerade auch durch die Einführung des Internets der Dinge, erfordern jedoch eine einheitliche Sichtweise, die Safety und Security parallel gewährleistet. So kann ein Hackerangriff, etwa durch die derzeit sehr „populäre" Ransomware, mit der IT-Systeme verschlüsselt und blockiert werden, ohne Weiteres die Betriebssicherheit einer Anlage beeinträchtigen. Auf der anderen Seite können Maßnahmen, die der Betriebssicherheit dienen, auch die Security herabsetzen. Aus dieser Erkenntnis sind in der jüngsten Zeit verstärkt Initiativen entstanden, Safety und Security gesamtheitlich zu betrachten.

Eine dieser Initiativen ist das TÜV AUSTRIA Research Lab for Safety and Security in Industry (#SafeSecLab), eine Kooperation zwischen der TU Wien und TÜV AUSTRIA. Neun vernetzte Einzelprojekte analysieren das Zusammenspiel und die gegenseitige Abhängigkeit der beiden Schutzziele im Kontext der industriellen Automatisierung, inklusive eines dafür notwendigen Bedrohungsmodells und davon abgeleiteten Risikomanagements. Das gemeinschaftliche Ziel aller Einzelprojekte ist es, Verfahren sowie technische und organisatorische Maßnahmen zu identifizieren, die Safety und Security industrieller Komponenten, Systeme und Anlagen entlang ihres gesamten Lebenszyklus gewährleisten.

Auch das vorliegende Schwerpunktheft zum Thema „Safety und Security" befasst sich mit integrierten und übergreifenden Ansätzen zur Sicherheitstechnik unter Berücksichtigung von Modellierungs-, Entwurfs- und Laufzeittechniken. Autor/innen aller Disziplinen waren eingeladen, ihre jüngsten Forschungsergebnisse oder Berichte vorzustellen, bei denen Safety und Security unter einem ganzheitlichen und vereinenden Blickwinkel betrachtet werden. Die Artikel beleuchten Sicherheit aus unterschiedlichen Blickwinkeln: von Industrie 4.0 (Fertigungstechnik und Prozessautomatisierung) über Automated Driving hin zu Entscheidungsprozessen, die durch böswillige Attacken beeinflusst werden können.

Der Beitrag von Siegfried Hollerer et al. gibt Einblicke in den aktuellen Umgang mit Safety und Security in der österreichischen Industrie bei ausgewählten Unternehmen des #SafeSecLab-Partnernetzwerks, die Komponenten im automatisierungstechnischen Umfeld herstellen, als Integratoren tätig sind oder selbst Automatisierungsanlagen betreiben. Die Ergebnisse der durchgeführten Befragung verdeutlichen einmal mehr die Notwendigkeit eines einheitlichen, ganzheitlichen Ansatzes, um Risiken hinsichtlich Security und Safety vollumfänglich erkennen und bewerten zu können.

Marco Ehrlich et al. untersuchen aus Sichtweise der Wissenschaft und Praxis eine mögliche Automatisierung von Risikobewertungsprozessen im Bereich der industriellen Automatisierung. Sie beschreiben dazu den aktuellen Stand der Technik bei der Bewertung von Sicherheitsrisiken und kommen zum Schluss, dass es einer gemeinsamen Taxonomie für beide Bereiche und eines abgestimmten Prozesses bedarf. Sie geben einen ersten Einblick in die dazu notwendige gemeinsame Formalisierung von Sicherheitsinformationen, die die Entwicklungen geeigneter digitaler Zwillinge und ihrer entsprechenden Teilmodelle unterstützen.

Florian Pelzer et al. stellen einen Demonstrator vor, der es ermöglicht, Aspekte der modulbasierten Produktion in der Prozessautomatisierung mit der dazu notwendigen Auslegung von Prozessmodulen im Hinblick auf deren funktionale Sicherheit zu untersuchen. Sie gehen der Fragestellung nach, wie Sicherheitssysteme technisch umgesetzt werden können, ohne die Flexibilität einer modularen Anlage einzuschränken. In ihrer Analyse gehen sie konform zu den beiden international wichtigen Normen der IEC 61508 und IEC 61511 vor. Der Beitrag gibt ebenso praktische Einblicke in den Aufbau und die Implementierung eines verteilten Safety Instrumented Systems, mit dem das Betriebspersonal zukünftig weitere Kompetenzen erwerben kann.

Christian Schwarzl et al. vom Virtual Vehicle Research Center in Graz zeigen, wie sich Security-Angriffe direkt auf die funktionale Sicherheit von Fahrzeugen auswirken können und dass es derzeit keinen akzeptierten Ansatz zur Kombination von funktionalen

Kastner, Wolfgang, Institute of Computer Engineering, Automation Systems, TU Wien, Wien, Österreich (E-Mail: k@auto.tuwien.ac.at); **Sauter, Thilo,** Institut für Computertechnik, TU Wien, Wien, Österreich; Department für Integrierte Sensorsysteme, Donau-Universität Krems, Krems, Österreich

Sicherheits- und Cybersicherheitsaktivitäten gibt. In ihrem Beitrag werden die im Automobilbereich bekannten Sicherheitsmethoden zusammengefasst und gemeinschaftliche Methoden zur Erreichung von funktionaler Sicherheit und Cybersicherheit im Analyse- und Entwurfsprozess erläutert sowie anhand der Testpattform SPIDER erprobt.

Der Artikel von David Schreiber et al. beschäftigt sich schließlich mit einem mehr IT-lastigen Aspekt bei der Sicherheit kritischer Infrastrukturen: dem Schutz gegen Desinformation und Fake News, speziell in sozialen Medien. Das Ziel ist die automatische Auswertung einer Vielzahl von Quellen zur Erkennung von Angriffen. Die dabei eingesetzten forensischen Methoden auf der Basis von künstlicher Intelligenz und maschinellem Lernen sind jedoch universeller und finden auch in anderen Bereichen Anwendung, um Attacken zu detektieren.

Als Gastherausgeber dieser e&i-Ausgabe zum Thema „Safety und Security" möchten wir uns an dieser Stelle sehr herzlich bei allen Autor/innen für ihre Beiträge und bei den Gutachter/innen für ihr geschätztes Feedback zu den jeweiligen Beiträgen bedanken. Unser spezieller Dank geht ebenso an die Redakteurinnen der e&i vom OVE Österreichischer Verband für Elektrotechnik für ihre umfangreiche Unterstützung.