Eine sichere Zukunft für die Robotik gewährleisten

Die Rolle der Cybersecurity

Autor:
Manoj Rajashekaraiah
Principal Engineer
Analog Devices
www.analog.com

Der Beitrag erläutert Cybersicherheitsrisiken und wirksame Maßnahmen zum Schutz von Robotersteuerungssystemen. Er umfasst industrielle Sicherheitsstandards und analysiert die wesentlichen Anforderungen, die zu erfüllen sind, um diesen Standards gerecht zu werden.

Einführung

Die Fabrikautomation steht im Zentrum von Industrie 4.0. Industrieroboter, autonome mobile Roboter (AMR) und kollaborierende Roboter (COBOTs) spielen eine entscheidende Rolle und ermöglichen es, die moderne Industrie 4.0 zu implementieren. Roboter werden intelligenter, kollaborativer und besser positioniert, um komplexe Aufgaben mit und ohne Eingriffe des Menschen zu erledigen.

Ein höherer Automatisierungsgrad und ein verstärkter Einsatz von Robotern führen zu einem gesteigerten Bedarf an höherer Funktions- und Datensicherheit von Robotersteuerungssystemen. Roboter wurden ursprünglich meist in Fabriken eingesetzt. Heute jedoch werden Roboter in verschiedenen Bereichen wie Medizin, Militär, Logistik und Landwirtschaft verwendet.

Der Bedarf an Funktions- und Datensicherheit ist heute viel wichtiger als noch vor zehn Jahren. Unfälle sind unvermeidbar. Doch diejenigen, die durch böswillige Angriffe verursacht werden, sind kritisch. Die böswillige Übernahme und Steuerung von Robotern kann ernsthafte wirtschaftliche und finanzielle Verluste verursachen.

Security-Risiken in Robotersteuerungssystemen

Bild 1 zeigt typische Cybersicherheitsrisiken, die bösartige Angriffen auf Robotersteuerungssysteme ermöglichen [7].

Einen Überblick über einige der Bedenken gibt Tabelle 1.

Vorschriften und Gesetze

für die Bereiche Industrie und Robotik fördern die Widerstandsfähigkeit gegenüber Cyberangriffen und sichern den Anlagenbetrieb. Die Cybersicherheitslandschaft entwickelt sich rasant, und es gibt eine wachsende Zahl von Vorschriften und Gesetzen für die Bereiche Industrie und Robotik. Zu den vielen Gesetzen hinsichtlich Cybersicherheit gehören der EU Cybersecurity Act [1], der EU Cyber Resilience Act [2] und das U.S. Cyber Incident Reporting for Critical Infrastructures Act [3]. Auch in China und Indien sind entsprechende Vorschriften und Gesetze am Entstehen.

Der NIST Guide to Operation Technology (OT) Security [4] und Normen wie IEC 62443 [5] bieten uns eine Orientierungshilfe und ermöglichen es uns, das Secure-by-Design-Konzept zu verfolgen und unsere Steuerungssysteme so zu gestalten und zu entwickeln, dass sie widerstandsfähig gegenüber Angriffen auf die Cybersicherheit sind.

Anforderungen der Norm IEC 62443

Beim internationalen Cybersecurity-Standard IEC 62443 geht es um Maßnahmen zum Schutz von industriellen Automatisierungs- und Steuerungssystemen (IACS) [6] vor böswilligen Angriffen. [8] IEC 62443 ist ein weit verbreiteter Standard für die Entwicklung von Steuerungssystemen für die Industrieautomation (Bild 2). Die meisten Bestimmungen empfehlen den Standard und erkennen seine Bedeutung an. Der Standard ermöglicht es, die entsprechenden Vorschriften einzuhalten, potentielle Cybersicherheitsrisiken in Steuerungssystemen zu vermindern, Sicherheitslücken in Steuerungssystemen zu adressieren, wichtige Anlagen zu schützen und vieles mehr.

Datensicherheit von Komponenten

Während sich einige Bereiche des Standards auf Prozesse und Verfah-

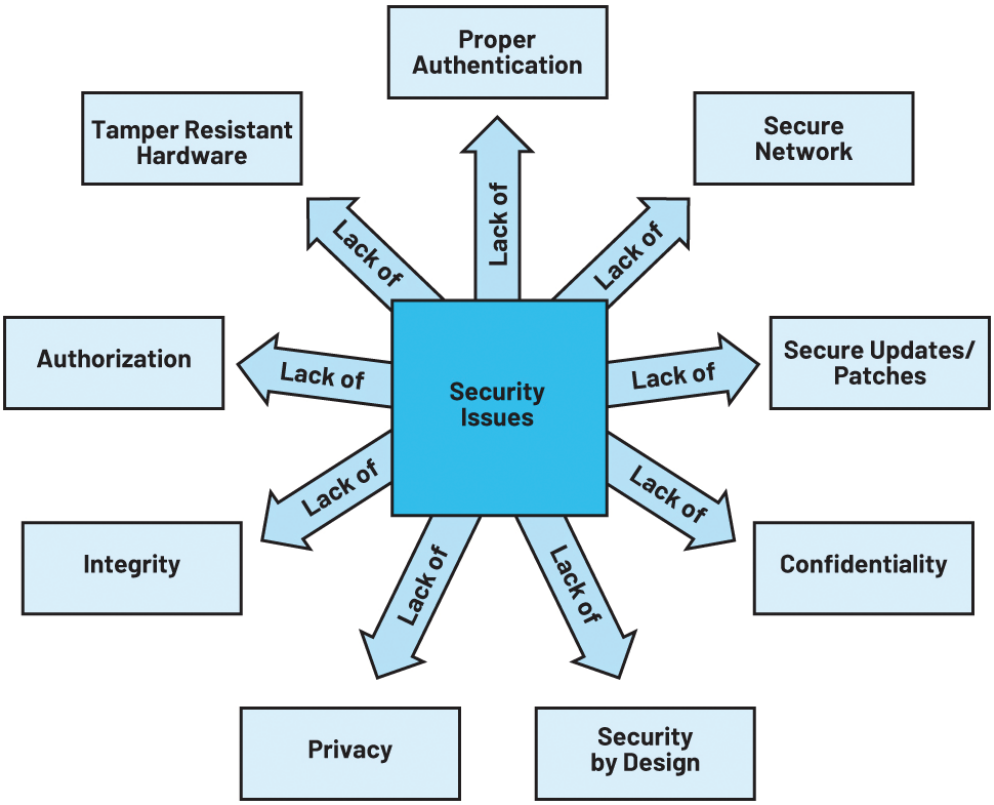

Bild 1: Security-Risiken in Robotersteuerungssystemen

ren konzentrieren, befassen sich die IEC 62443-4-1 und IEC 62443-4-2 speziell mit der Datensicherheit von Komponenten. Komponententypen gemäß IEC 62443-4-2 sind Softwareanwendungen, Hostgeräte, Embedded Geräte und Netzwerkgeräte. Der Standard definiert die Sicherheitsstufe (SL) für jeden Komponententyp auf der Basis der Komponentenanforderung (CR) und der Anforderungserweiterung (RE), die sie erfüllen. Der Standard definiert vier Sicherheitsstufen (SL) SL0 bis SL3. Die Stufen SL2 und SL3 erfordern insbesondere hardwarebasierte Datensicherheit.

Fähigkeiten und Technologien

Welche Fähigkeiten und Technologien sind für die Entwicklung von Security-Systemlösungen für Roboter erforderlich?

Um sichere Robotersteuerungssysteme zu entwickeln, müssen wir die Risiken adressieren, die im Abschnitt Security-Risiken in Robotersteuerungssystemen hervorgehoben werden. Zu den wichtigsten erforderlichen technischen Fähigkeiten und Technologien gehören:

- **Sichere Authentifizierung**: Integration von sicheren Authentifikatoren, um die Identität von Geräten/Komponenten nachzuweisen.
- **Sichere Coprozessoren**: Nutzung von dedizierter Hardware für die sichere Speicherung und kryptografische Operationen.
- **Sichere Kommunikation**: Implementierung von verschlüsselten Protokollen für geschützten Datenaustausch.
- **Zugriffskontrolle:** Durchsetzung granularer Berechtigungen zur Einschränkung unbefugter Systemzugriffe.
- **Physikalische Sicherheitsmaßnahmen**: Implementierung von Maßnahmen zum Schutz vor physikalischer Sabotage.

Schlüsselfertige Security-ICs

wie beispielsweise sichere Authentifikatoren und Coprozessoren, wurden speziell für diese Anforderungen entwickelt und bieten eine einfache Implementierung und Kosteneffizienz. Diese ICs mit fester Funktion werden durch umfassende Software-Stacks ergänzt, die für Host-Prozessoren entwickelt wurden. [8]

Hinweis: Die Verwendung eines diskreten sicheren Elements (SE) erhöht die Widerstandsfähigkeit des Systems, indem es einen kompromittierten Anwendungsprozessor daran hindert, auf Zugangsdaten zuzugreifen, die in einem separaten IC gespeichert sind (Isolierung).

Strukturierter Ansatz

Zusätzlich zu diesen Aspekten müssen Systementwickler einem strukturierten Ansatz für die sichere Entwicklung folgen. Dieser muss folgendes beinhalten: Anforderungserfassung, Bedrohungsmodellierung, sicheres Design, Implementierung, Prüfung, Zertifizierung und Wartung. Die Einhaltung eines sicheren Entwicklungsprozesses (SDL) sorgt dafür, dass Datensicherheit von Anfang an in den Entwicklungsprozess integriert ist.

Beispiel-Anwendungsfall in einer Robotergelenksteuerung

Ein mögliches Systemdesign für eine Robotergelenksteuerung innerhalb eines Robotergelenks zeigt Bild 3.

In diesem Design wird das Anwendungspotential des MAXQ1065 deutlich, da das Bauteil die Implementierung einer sicheren Boot-Funktionalität ermöglicht und damit die Gesamtdatensicherheit des Systems erhöht. Es bietet ferner eine Reihe zusätzlicher Leistungsmerkmale, wie beispielsweise sichere Schlüsselspeiche-

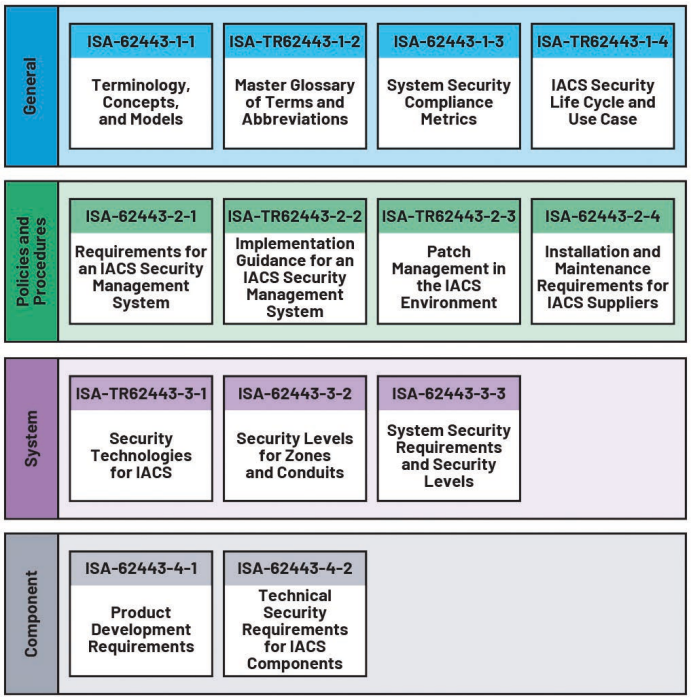

Bild 2: IEC 62443 ist ein umfassender Security-Standard

Mangel an	Auswirkung und Beschreibung
Sichere Vernetzung	Macht die Kommunikation zwischen Robotersteuerungssystemen unsicher und anfällig für Spoofing-Angriffe, Manipulationen und Abhören. Dies kann sich auch auf die Verfügbarkeit des Systems auswirken.
Korrekte Authentifizierung	• Dies führt zu unberechtigtem Zugriff mit Standardbenutzernamen und -passwörtern. • Eine fehlende Authentifizierung von Geräten oder Peripheriegeräten ermöglicht den Einsatz von gefälschten Peripheriegeräten/Zubehörteilen in Robotersystemen, die Funktions- oder Datensicherheitsrisiken darstellen. • Führt auch dazu, dass Dateneingaben aus nicht vertrauenswürdigen, nicht identifizierten Quellen akzeptiert werden.
Vertraulichkeit	Fehlende Verschlüsselung oder schwache Verschlüsselungsalgorithmen führen dazu, dass sensible Roboterdaten und Designpläne abgefangen und offengelegt werden können.
Integrität	Dies kann dazu führen, dass sensible Roboterdaten, Konfigurationen und Firmware verändert werden, die entweder gespeichert oder in Übertragung sind.
Secure Boot und Update	• Ohne dies können wir nicht sicher sein, ob auf unserem Robotersteuerungssystem authentische Firmware/Software arbeitet. • Das Fehlen von sicheren Updates könnte das Eindringen in Robotersteuerungssysteme ermöglichen, indem entweder ein Rollback auf anfällige ältere Software durchgeführt oder nicht authentische Software in Robotersteuerungssysteme programmiert wird.
Manipulationssichere Hardware	Manchmal speichern Roboter extrem sensible Informationen (z. B. Roboter, die im Militär/Verteidigungsbereich eingesetzt werden). Es ist sehr wichtig, diese Informationen vor dem Zugriff durch unbeabsichtigte Akteure zu schützen. Ohne manipulationssichere Hardware wird es schwierig, Informationen vor invasiven Angriffen zu schützen.
Secure by Design	Die meisten Steuerungssystementwicklungen basierten bis vor kurzem nicht auf dem Prinzip des „Secure by Design“. Dies kann ein Eindringen in die Architektur und das Design des Robotersystems ermöglichen, um dessen Schwachstellen herauszufinden und für einen Angriff auszunutzen.
Updates	Fehlende Updates für Betriebssystem, Firmware und Robotersoftware können Cyberangriffe ermöglichen.

Anmerkung: Ein erheblicher Teil der Security-Risiken entsteht aufgrund von Software-Schwachstellen.

Tabelle 1: Bedenken bezüglich Security-Risiken

rung, sichere Kommunikationsprotokolle und kryptografische Operationen. In Folgeartikeln werden diese Anwendungsfälle und ihre praktischen Einsatzmöglichkeiten näher beleuchtet.

Zusammenfassung

Um die Zukunft der Robotik sicherzustellen, ist die Cybersicherheit von zentraler Bedeutung. Verlässliche Maßnahmen wie sichere Authentifizierung, verschlüsselte Kommunikation und Datensicherheit in der Lieferkette sind entscheidend für den Schutz vor Bedrohungen.

Durch Priorisierung von Cybersicherheit und die Nutzung des Know-hows erfahrener Partner, kann das volle Potential der Robotik ausgeschöpft werden und zugleich vor neuen Risiken in einer vernetzten Welt schützen.

Links

[1] EU Cybersecurity Act: https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/cybersecurity-network-and-information-security-rp-2023

[2] EU Cyber Resilience Act: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf

[3] U.S. Cyber Incident Reporting for Critical Infrastructures Act: https://www.cisa.gov/sites/default/files/2023-01/Cyber-Incident-Reporting-ForCriticalInfrastructure-Act-of2022_508.pdf

[4] NIST Guide to Operation Technology (OT) Security: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf

[5] IEC 62443: https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards

[6] IACS: https://www.analog.com/en/signals/thought-leadership/the-iec-62443-series-of-standards-how-to-defend.html

Literatur

[7] Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, und Ali Chehab. “Robotics Cyber Security: Vulnerabilities, Attacks, Countermeasures, and Recommendations.” International Journal of Information Security, März 2021.

[8] Christophe Tremlet. “The IEC 62443 Series of Standards: How to Defend Against Infrastructure Cyberattacks.” Analog Devices Inc., April 2023.

Wer schreibt:

Manoj Rajashekaraiah ist ein Principal Engineer und hat sich auf das Design von Softwaresystemen innerhalb der Security Business Unit von Analog Devices spezialisiert. Mit einem starken Fokus auf Embedded Device Security zeichnet er sich durch die Entwicklung von Safety-, Security- und Sensorsoftware für Automobil- und IoT-Anwendungen aus. ◄

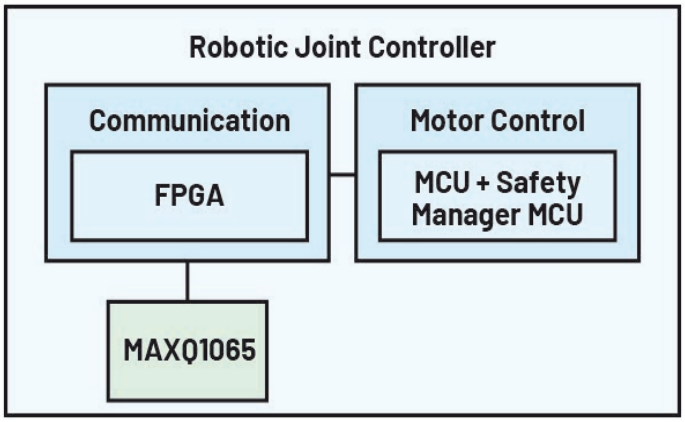

Bild 3: Möglicher Einsatz des MAXQ1065 in einem Robotergelenksteuerungssystem