Mit den embedded Kommunikationsschnittstellen Anybus CompactCom können Gerätehersteller nicht nur die Netzwerkanbindung für ihre Geräte an industrielle Netzwerke realisieren. Beim Einsatz von Anybus CompactCom IIoT Secure können sie ihr Gerät außerdem mit deutlich reduziertem Aufwand auf ein höheres Sicherheitsniveau bringen.

Cybersecurity in der industriellen Automation

Keywords
- *Anlagensicherheit*
- *Cybersecurity*
- *Automatisierung*

Mehr Vernetzung von Anlagen erfordert neue Sicherheitsmaßnahmen

Cybersecurity wird in der industriellen Automation ein immer dringlicheres Thema. Einerseits steigt durch die zunehmende Vernetzung von Anlagen und Anlagenteilen die Anfälligkeit für Cyberangriffe auf Systeme. Andererseits fordern immer mehr rechtliche Vorgaben wie NIS2 oder der Cyber Resilience Act entsprechende Maßnahmen. Der Stand in Sachen Cybersecurity bei den verschiedenen industriellen Kommunikationsstandards ist jedoch sehr unterschiedlich. Heterogene Netzwerkinfrastrukturen bekommen zusätzlich eine hohe Komplexität bezüglich rechtlicher Vorgaben und technisch verfügbarer Lösungen für Cybersecurity.

Immer häufiger auftretende Angriffe auf Industrieanlagen, auch bedingt durch die fortschreitende Vernetzung, lassen die Sicherheit von OT-Netzwerken zunehmend zu einer Frage der Wirtschaftlichkeit werden. Dieser Umstand und neue rechtliche Vorgaben wie NIS2 oder der Cyber Resilience Act, in denen die EU klare Cybersicherheitsanforderungen definiert, bringen Unternehmen jetzt in Zugzwang. Denn der Ablauf der Übergangsfristen ist in sichtbare Nähe gerückt. Aber die Automatisierungswelt ist komplex, oft sind Netzwerkarchitekturen heterogen und nutzen zudem verschiedene Kommunikationsstandards. Die wiederum sind im Hinblick auf Cybersecurity unterschiedlich weit gereift. Was können Gerätehersteller, Maschinenbauer oder Anlagenbetreiber kurzfristig tun? Was sollten sie mittel- und langfristig unternehmen?

Stand heute sind in den wenigsten Automatisierungsgeräten, die in Produktionsanlagen im Einsatz sind, Cybersecurity-Funktionen integriert. Zu gering war bislang der Druck. Das ändert sich, wie eingangs beschrieben. Eine robuste Cybersecurity-Strategie wird zur rechtlichen Anforderung, denen Geräte- und Maschinenbauer sowie Anlagenbetreiber nachkommen müssen. Beispielsweise trat die EU-Richtlinie NIS2 bereits 2023 in Kraft, die Umsetzung in nationales Recht sollte im Oktober 2024 erfolgt sein, zieht sich voraussichtlich aber noch bis März 2025 hin. Nicht nur Unternehmen aus

Schon heute gibt es verschiedene Tools für eine sichere Anlagenkommunikation: Anybus Atlas für kontinuierliche Netzwerkdiagnose, Anybus Defender als Firewalls für die Steuerung und Überwachung der Kommunikation sowie Anybus Gateways zur logischen und physikalischen Segmentierung von Netzwerken.

dem klassischen KRITIS-Bereich sind davon betroffen, sondern auch Unternehmen aus der Industrie. Insbesondere für Anlagenbetreiber sind die neuen Security-Anforderungen durch NIS2 relevant, da es darum geht, die Sicherheit von Netzwerken und Informationssystemen zu gewährleisten. Im Dezember 2024 trat außerdem der Cyber Resilience Act (CRA) in Kraft, der Security-Anforderungen an Geräte und Maschinen definiert, die auf dem EU-Markt erhältlich sind. Die Umsetzungsfrist läuft bis 2027. Ab diesem Zeitpunkt dürfen in Europa nur noch cyber-sichere Geräte in Umlauf gebracht werden.

Herausforderung: Technologievielfalt

Anders als in IT-Netzwerken, die gewöhnlich auf einheitlicherem Standard sind, weil sich dort Technologien in kürzeren Zyklen konsolidieren, sind industrielle Netzwerke auf Fertigungsebene wegen der dort herrschenden Technologievielfalt deutlich komplexer. Unterschiedliche Netzwerkarchitekturen und Kommunikationslösungen wurden über Jahrzehnte in den Produktionsstandorten installiert. Heute erfordert die zunehmende Digitalisierung nicht nur die stärkere Vernetzung bisheriger Insellösungen, sondern bringt auch zusätzliche Technologien wie z.B. OPC UA mit sich, die für die IoT-Kommunikation gebraucht werden. Darüber hinaus muss die industrielle Kommunikation reibungslos funktionieren, ohne Abstriche bei Determinismus oder Performanz. All das ist an sich schon Herausforderung genug. Doch jetzt kommt noch Cybersecurity hinzu. Dass die Sicherheitserweiterungen der einzelnen Kommunikationsprotokolle wie Profinet Security, CIP Security für EtherNet/IP, Modbus TCP Security oder OPC UA Security technisch auf verschiedenen Leveln und zum Teil noch gar nicht einsetzbar sind, macht die Thematik nicht gerade einfacher.

Die Security-Erweiterung für OPC UA war bereits in den ersten Spezifikationen (2006) enthalten, und wird bis heute ständig verbessert. Die verschiedenen Kommunikationsmechanismen im OPC-UA-Standard erfordern unterschiedliche Ansätze (https, Websocket, TLS, …). Diese Sicherheitsfunktionen werden heute bereits in ersten Anwendungen eingesetzt, da OPC UA oft für die Anbindung an die IT-Welt benutzt wird. Die Praxis hat allerdings gezeigt, dass die neuen Sicherheitsmechanismen noch nicht automatisch abgewickelt werden können. Security-Zertifikate müssen beispielweise nach Ablauf immer noch von Hand aktualisiert werden.

CIP Security für EtherNet/IP wurde erstmals im Jahr 2016 spezifiziert und die Anwendbarkeit auf Systemebene wurde über die Jahre erweitert. Da das Protokoll auf standardisierten Mechanismen basiert, wird die Sicherheit durch die anerkannten TLS/DTLS-Protokolle und x.509-Zertifikate gewährleistet. Erste Engineering-Tools und Produkte werden bereits von führenden Anbietern angeboten, jedoch ist die Marktakzeptanz bislang eher verhalten.

Die Security Erweiterung für Profinet hingegen wurde zwischen 2021 und 2024 verhältnismäßig spät spezifiziert. Es gibt drei Security-Klassen, die jeweils den Integritätsschutz der GSD-Dateien, den Integritätsschutz der Kommunikation und die Vertraulichkeit der Kommunikation spezifizieren. Derzeit arbeiten Technologielieferanten noch an einer ersten Umsetzung und validieren die Interoperabilität zwischen Lösungen verschiedener Hersteller im Hinblick auf die neuen Sicherheitsfunktionen.

Und das sind nur drei der vielfältigen am Markt verbreiteten Kommunikationsstandards, die sich alle im Hinblick auf ihre Sicherheitskonzepte, ihre Technologiereife und dafür vorhandene Ökosysteme unterscheiden. Das bedeutet für Gerätehersteller, Maschinenbauer und Anlagenbetreiber eine wahre Sisyphus-Aufgabe: Sie müssen stets den Überblick wahren über verschiedene rechtliche Vorgaben einerseits und vorhandene technische Lösungen andererseits.

Heute Geräte für morgen bauen

Langfristig wird Cybersecurity von den Herstellern in alle Geräte, Maschinen und Anlagen integriert werden. Dieser Weg ist weit und braucht Zeit. Sehr kurzfristiger Handlungsbe-

darf besteht übrigens bei den Herstellern von Wireless-Geräten. Diese dürfen ab 2025 ohne Erfüllung der Anforderungen der europäischen Radio Equipment Directive (RED), die eben auch deren Cybersecurity betreffen, nicht mehr auf den Markt gebracht werden.

Aber auch alle anderen Gerätehersteller, die eine digitale Kommunikationsschnittstelle integrieren müssen, stehen schon jetzt vor der herausfordernden Aufgabe, zukunftsfähige Geräte in Sachen Cybersecurity zu bauen. Dazu sollten sich Gerätebauer mit dem Cyber Resilience Act (CRA) befassen. Spannend ist dabei, dass diese Vorgaben noch relativ neu sind und ihre Umsetzung in der Praxis erst reifen muss. Im Rahmen des CRA wird Cybersecurity integraler Bestandteil der Geräteentwicklung. Dies umfasst die Spezifikation, die Dokumentation für den fachgerechten Einsatz im Feld sowie die Produktpflege. Letztere muss gewährleisten, dass über den gesamten Lebenszyklus hinweg bekannte Sicherheitslücken in Geräten geschlossen und auch zukünftige Schwachstellen behoben werden. All das wird auch die Unternehmensprozesse, insbesondere im Bereich Produktentwicklung und Produktmanagement, stark verändern.

Die IEC 62443 beschreibt in Teil 4-1 den Rahmen, innerhalb dessen Komponentenhersteller bzw. Automatisierungsgerätehersteller ihre Prozesse entsprechend strukturieren sollten. Teil 4-2 des Standards legt die Anforderungen für die Komponenten selbst fest. Damit dient er als Leitfaden, um in Unternehmen mittel- und langfristig eine cybersichere Herangehensweise zu etablieren. Eine Zertifizierung stellt den Nachweis für entsprechende Maßnahmen für mehr Cybersicherheit dar.

Cybersecurity kurzfristig in Geräte integrieren

Für die in Geräten eingesetzten Kommunikationskomponenten führt das aus Sicht von HMS zu zwei wesentlichen Maßnahmen. Einerseits muss die Hardware bereits jetzt so dimensioniert sein, dass bspw. der Prozessor über die notwendige Leistung verfügt, um künftige Sicherheitsaufgaben wie Verschlüsselung, Authentifizierung, Benutzerverwaltung oder Zertifikatsmanagement verarbeiten zu können. Andererseits muss es möglich sein, Änderungen nachträglich automatisch aufzuspielen, um eine robuste Cybersecurity-Strategie kontinuierlich an den veränderten Ist-Zustand anzupassen. Die Zusatzkosten für die komplexere Hardware konnten Gerätebauer bislang schwer rechtfertigen. Mit der veränderten Gesetzeslage führt aber kein Weg am Einsatz vorbei, will man zukunftssichere Geräte bauen.

Die Kommunikationsexperten von HMS bieten bereits Lösungen, mit denen sich Cybersecurity kurzfristig in Geräte integrieren lässt. Thierry Bieber, Industry Manager, HMS Industrial Networks erläutert: „Wir verstehen uns als Technologiepartner, der bei der Security Compliance und Pflege unterstützt. Wir nehmen Kunden die Aufgabe ab, stets auf dem neuesten Stand der Technik sein zu müssen. Unsere embedded Kommunikationsschnittstellen haben schon IIoT- und Cybersecurity-Funktionen implementiert. Damit bieten wir Geräteherstellern insbesondere im Hinblick auf die Security-Erweiterungen der Kommunikationsprotokolle eine einsatzbereite zukunftssichere Lösung."

Mehr Sicherheit für Automatisierungsgeräte mit Anybus CompactCom IIoT Secure.

Das Kommunikationsmodul Anybus CompactCom IIoT Secure verfügt über eine sichere Verwaltung der Zertifikate, die für die verschlüsselte Kommunikation verwendet werden. Vertrauliche Daten wie z.B. private Schlüssel werden auf einem separaten Sicherheits-Chip gespeichert. Beim sicheren Booten wird auch geprüft und gewährleistet, dass nur signierte Software von HMS verwendet wird. Darüber hinaus verschlüsseln die Sicherheitsfunktionen des Moduls die IIoT-Datenverbindungen (OPC UA & MQTT) und unterstützen auch die Sicherheitsanforderungen der jeweiligen industriellen Protokolle. Gerätehersteller, die bereits ein embedded Kommunikationsmodul für Profinet oder EtherNet/IP nutzen, können mit dem Anybus CompactCom IIoT Secure ihr eigenes Geräteportfolio mit deutlich reduziertem Aufwand auf ein höheres Sicherheitsniveau bringen.

Kurzfristige Lösungen für Instandhalter und Anlagenbetreiber

Auch Anlagenbetreiber stellen sich die Frage, was sie heute schon tun können. Für sie interessant ist vor allem die NIS2-Richtlinie. Bis Cybersecurity vollständig in Geräte integriert wird und diese neuen Gerätegenerationen bei den Anlagenbetreibern ankommen, werden vermutlich noch Jahre vergehen.

Deshalb ist es für Anlagenbetreiber wichtig, sich schon heute einen umfassenden Überblick über ihre Produktionsinfrastrukturen zu verschaffen, die oft über Jahrzehnte gewachsen sind. Kritische Maschinen und Anlagenteile müssen identifiziert und in sichere Netzwerksegmente isoliert werden. Die einzelnen Kommunikationszugänge müssen permanent überwacht werden, um sicherzustellen, dass nur autorisierter Datenverkehr stattfindet. Externe und unerlaubte Zugriffe können so verhindert werden, was schon einen effizienten Schutz in einem an sich nicht sicheren Netzwerk bietet.

Firewalls wie der Anybus Defender ermöglichen es, durch Regeln unerlaubte Zugriffe auf Netzwerksegmente zu verhindern und den Datenverkehr zu überwachen. Mit Produkten aus dem Bereich der Anybus Gateways wird eine logische und physikalische Segmentierung von Netzwerken realisierbar. Anybus Atlas und die Osiris Software werden für die kontinuierliche Diagnose und die Erkennung von Anomalien im Datenverkehr eingesetzt.

Wer darüber hinaus den Fernzugriff mit den Ewon-Fernwartungslösungen von HMS standardisiert, kann für die Zusammenarbeit mit externen Lieferanten einheitliche Prozesse aufsetzen, um bei Netzwerkzugriffen von außen die volle Kontrolle zu behalten und damit ein hohes Maß an Sicherheit zu erreichen. Große Automatisierungsunternehmen befassen sich derzeit umfangreich mit dem Thema Cybersecurity und spüren: Die Zeit wird knapp. Ein Technologiepartner wie HMS kann dabei wertvoller Unterstützer sein, indem er die Implementierung von Spezifikationen in entsprechende Hardware übernimmt und direkt einsatzfähige, stets aktuelle und Cybersecurity konforme Kommunikationslösungen anbietet.

Thilo Döring,
Geschäftsführer,
HMS Industrial Networks

Wiley Online Library

HMS Industrial Networks GmbH, Karlsruhe
Tel.: +49 721 989777-000
info@hms-networks.de · www.hms-networks.de