Strategien zur IIoT- und Security-Implementierung in Automatisierungsgeräte

Security als Wettbewerbsvorteil nutzen

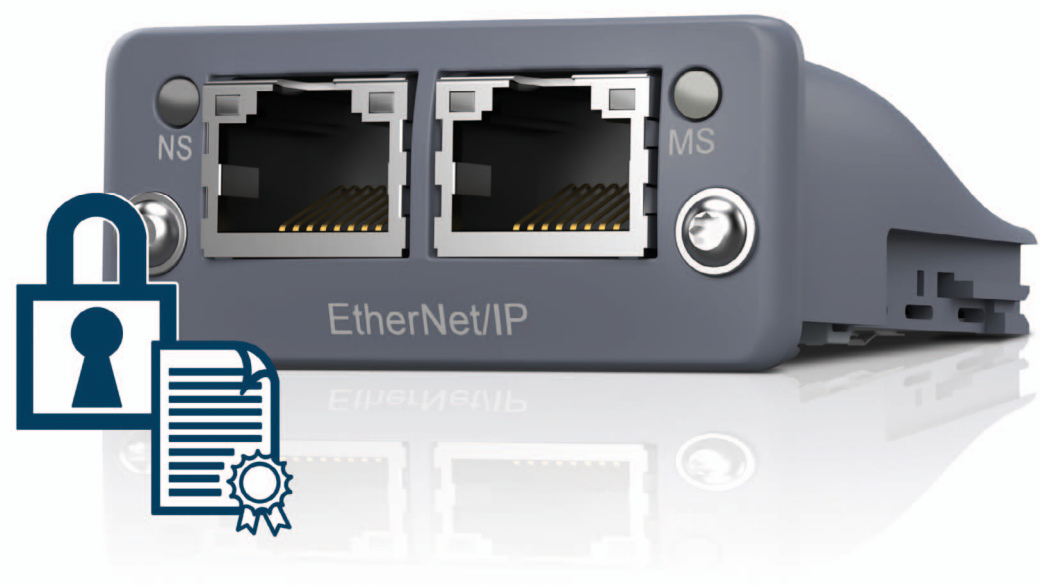

Bild 1: Das Anybus-Kommunikationsmodul von HMS wickelt zusätzlich zur Buskommunikation auch die Kommunikation via OPC UA und MQTT ab. ©HMS

Die digitale Transformation verändert die Fertigung grundlegend mit dem Ziel, auf Basis der Fertigungsdaten einen Mehrwert zu schaffen, der Grundlage für neue Geschäftsmodelle sein kann. Ethernet als Kommunikationsstandard setzt sich dabei immer mehr durch und IT- und OT-Ebene konvergieren. Die Interaktion nimmt zu. Dadurch gewinnt das Thema Cybersecurity zunehmend an Bedeutung, also der Schutz vor unautorisierten Zugriffen und Bedrohungen. Das gilt im Netzwerkverbund für jedes einzelne Automatisierungsgerät. Hier müssen die Hersteller aktuelle und zukünftige Standards unterstützen und sichere Schnittstellen implementieren. Dazu ist Expertenwissen erforderlich. Zeit in die eigene Lernkurve zu investieren rechnet sich in den seltensten Fällen. Modulare Lösungen machen es möglich, Cybersecurity deutlich schneller und technisch auf höchstem Niveau in die eigene Applikation zu integrieren und sich so Wettbewerbsvorteile zu sichern.

Sichere Kommunikationsschnittstelle zum IoT

Hersteller von Automatisierungsgeräten müssen im Zuge der fortschreitenden Digitalisierung nicht nur den zyklischen Austausch von Fertigungsdaten in ihre Kommunikationsschnittstelle integrieren, sondern auch die Anbindung an IoT-Plattformen. Die Herausforderung im IoT-Umfeld besteht insbesondere darin, eine Kommunikationsschnittstelle zu realisieren, die die Anbindung an die IoT-Plattform ermöglicht, ohne die von der industriellen Anwendung geforderte Sicherheit und Leistung zu beeinträchtigen. Hierbei gilt es neue Cybersecurity-

Bild 2: Das Thema Cybersecurity wird auch in der Fertigung zunehmend wichtiger. © Bildcollage mit shutterstock_602455865 und starline / Freepik 26024

Autor:
Thierry Bieber, Industrie Segment Manager Industrial Automation
HMS Industrial Networks GmbH
info@hms-networks.de
www.hms-networks.de

Anforderungen umzusetzen, die in ebenfalls neue IEC- oder Protokollstands einfließen, wie die IEC 62443, die den Rahmen für Security-Implementierungen bildet.

IIoT-Kommunikation innerhalb der Produktionsanlage

Um innerhalb einer Produktionsanlage von der IT-Ebene auf die Daten von Robotern, Antrieben, Sensoren oder I/O-Modulen zuzugreifen, setzen sich mit OPC UA und MQTT zwei Kommunikationsstandards durch. Beide Technologien haben jeweils ihren eigenen Schwerpunkt. OPC UA fokussiert auf die Standardisierung der Datenmodelle in Geräten der gleichen Familie – wie zum Beispiel Roboter, Bildverarbeitungssysteme, usw. – für eine einfache Integration bei Endkunden. MQTT ist ein sehr schlankes („lightweight") Protokoll, das schnell und einfach auch in kleinste Geräte implementiert werden kann, dafür aber keine standardisierte Datenmodellierung bietet. Beide Technologien haben ihre Anhänger, aber auch verschiedene Einsatzbereiche. Hersteller von Automatisierungsgeräten müssen deshalb eigentlich beide Protokolle implementieren, um alle ihre Anwender zufriedenzustellen. Das ist in der Praxis aufwendig und kostet Zeit.

Als einer der führenden Anbieter von Lösungen für die industrielle Kommunikation sowie das IIoT kann HMS Industrial Networks Anwender auch bei der Implementierung der benötigten IIoT-Schnittstellen unterstützen. Für die Produktreihe Anybus CompactCom, eine Familie von embedded Kommunikationsschnittstellen, wurde ein IIoT-Secure-Modul entwickelt, das sowohl Feldbus- als auch OPC UA- und MQTT-Protokolle integriert. Die Software-Schnittstelle zwischen dem Modul und dem Applikationsprogramm des Automatisierungsgerätes ist standardisiert. Somit haben Hersteller, die bereits ein Anybus-Modul für die Buskommunikation einsetzen, keinen zusätzlichen Aufwand, um Daten über OPC UA und MQTT zu übertragen. Beide Protokolle wurden sicher implementiert und erfüllen somit auch die notwendigen Cybersecurity-Anforderungen. Damit bietet HMS Geräteherstellern eine einfache und schnelle Möglichkeit, ihre Geräte auch ohne Expertenwissen IIoT-fähig zu machen.

Bild 3: Eine sichere Infrastruktur braucht einen mehrstufigen Ansatz bis hinunter auf die Komponentenebene. © Bildcollage mit shutterstock_1287262270 und shutterstock_1194038272

Neue industrielle Cybersecurity-Anforderungen

Mit dem steigenden Kommunikationsbedarf im industriellen Bereich nimmt auch die Anzahl der Cyber-Attacken in diesem Segment zu. Diese Attacken werden immer präziser und erfolgen jetzt auch über industrielle Protokolle. Die Folgen können dramatisch sein: Wasser- oder Energieversorgung können unterbrochen, die Funktionale Sicherheit in Anlagen kann umgangen werden. Deswegen arbeiten die unterschiedlichen Nutzerorganisationen an neuen Sicherheitskonzepten.

Die Modbus Organization hat dafür 2018 eine Modbus-Security-Erweiterung publiziert, um die Kommunikation zu verschlüsseln. Die ODVA hat die EtherNet/IP-Kommunikation 2015 um CIP Security erweitert. Die Spezifikation wird ständig verbessert, um die Implementierung dieser Sicherheitsprozesse für die Anwender einfacher zu machen. Die Robustheit und der Determinismus der Feldbusschnittstelle ist für die nahtlose Steuerung einer kritischen Anlage essenziell. Auch bei der Profibus Nutzerorganisation (PNO) ist das Thema Security stark im Fokus, und die PNO hat 2020 eine erste Sicherheitsklasse (Security Class) vorgestellt, die diese Robustheit garantiert.

Sichere Implementierung

Aber auch die Sicherheit der Geräte selbst muss berücksichtigt werden. Eine sichere Kommunikation ist nutzlos, wenn Unbefugte vertrauliche Gerätezertifikate lesen oder diese durch Manipulation der Firmware austauschen können. Die IEC62443-4-1 und -2 beschreiben einen Rahmen dafür, wie Komponentenhersteller bei einer sicheren Implementierung vorgehen müssen. Der erste Teil umfasst den Entwicklungsprozess bis hin zum gesamten Lebenszyklus des Gerätes, der zweite Teil beschreibt die Sicherheitsanforderungen an die Geräte.

Einhaltung der IEC62443

Bei HMS stellen wir fest, dass unsere Kunden in Projekten die Einhaltung der IEC62443 immer stärker fordern. Daher hat HMS diese Sicherheitsverfahren in seine Entwicklungsprozesse integriert und im IIoT-Secure-Modul modernste Sicherheitsfunktionen implementiert. Das Modul verfügt über eine sichere Verwaltung der Zertifikate, die für die verschlüsselte Kommunikation verwendet werden. Vertrauliche Daten wie zum Beispiel private Schlüssel werden auf einem separaten Sicherheits-Chip gespeichert. Beim sicheren Booten wird auch geprüft und sichergestellt, 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.

Fazit

Für Hersteller von Automatisierungsgeräten bedeutet das: Wenn sie auf die HMS-Lösung setzen, können sie ohne umfassende Sicherheitskompetenzen ein hohes Security-Niveau in ihren Geräten unterstützen. Und in einem Markt, in dem das Thema Security gerade mal in den Startlöchern steht, kann das ein entscheidender Wettbewerbsvorteil sein. Auch im Hinblick auf eine zukunftssichere Lösung. Denn HMS versteht sich als Technologiepartner, der seine Kunden langfristig begleitet. ◄

Weitere Informationen unter: https://www.anybus.com/de/produkte/embedded-index/security
Es gibt auch ein Whitepaper (Englisch) zum Thema:
https://www.hms-networks.com/technologies/iot-security/whitepaper-security-for-industrial-devices