Keywords
- *Manufacturing-X*
- *Datensicherheit, Security*
- *OPC UA*

© ANDREI – stock.adobe.com / generiert mit KI

Umfassend zugriffssicher

IEC62443-zertifizierte Automatisierungsplattform mit OPC UA Standard

Manufacturing-X steht für die Idee einer dezentralen Datenwirtschaft; Ziel ist es, Nachhaltigkeit, Wettbewerbsfähigkeit und Widerstandsfähigkeit durch die zugriffssichere Digitalisierung der Lieferketten zu erhöhen

Eine effiziente und nachhaltige Produktion ist zunehmend auf aktuelle Informationen angewiesen. Diese reichen von Störungen in den Lieferketten über die Rohstoff- und Energieversorgung bis zum Update Management der eingesetzten Geräte. Die Initiative Manufacturing-X zielt auf eine digital vernetzte Industrie mit einem standardisierten Datenaustausch über Unternehmens- und Branchengrenzen hinweg ab. Diese Kommunikation muss zwingend vor unbefugten Zugriffen abgesichert werden.

Bei PLCnext Technology handelt es sich um eine Plattform mit offener Architektur für die Industrieautomatisierung, die Anwendern eine sichere und robuste Umgebung für ihre Applikationen bietet. Die Plattform basiert auf dem internationalen Security-Standard IEC 62443, der für die Sicherheit von industriellen Steuerungssystemen sorgen soll. PLCnext Technology war das erste Ecosystem für die industrielle Automation, das im Jahr 2021 gemäß IEC 62443-4-1 ML3 und IEC 62443-4-2 mit SL2 zertifiziert worden ist. Hinter der Norm verbirgt sich ein umfassender Satz von Anforderungen, die dem Schutz industrieller Steuerungssysteme vor unberechtigten Zugriffen, böswilligen Attacken und anderen Sicherheitsbedrohungen dienen. Der Standard deckt alle Aspekte der Sicherheit inklusive der Authentifizierung, Autorisierung, Datenverschlüsselung und des Systemdesigns ab. Durch die Zertifizierung nach IEC 62443 erhalten die Anwender die Gewissheit, dass ihre Applikationen sicher und zuverlässig arbeiten.

Dreiklang aus Zugriffskontrolle, Authentifizierung und Verschlüsselung

Die Plattformtechnologie beinhaltet eine Reihe von Funktionen, die zur Absicherung von Anwendungen beitragen. Dazu gehören die Zugriffskontrolle, Authentifizierung und Verschlüsselung. Die Zugangskontrolle stellt sicher, dass lediglich autorisierte Benutzer auf das System zugreifen können. Im Rahmen der Authentifizierung müssen sie gültige Anmeldedaten angeben, um Zugang zum System zu bekommen. Die Verschlüsselung verhindert, dass unbefugte Benutzer Daten abfangen, die zwischen den Anwendungen und der PLCnext-Steuerung übertragen werden. Die Technologie stellt den Nutzern außerdem eine sichere Umgebung für die eigenen Applikationen zur Verfügung. Die Plattform ist so konzipiert, dass sie bösartige Angriffe – bspw. Viren und Malware – abwehrt. Sie umfasst darüber hinaus einen starken Schutz gegen Datenverlust und -manipulation.

OPC UA zur sicheren Aktualisierung von Geräten

Zum sicheren, zuverlässigen und robusten Datenaustausch zwischen industriellen Automatisierungsgeräten nutzt die Plattform zudem das Kommunikationsprotokoll OPC UA. Der Standard schafft eine zusätzliche Sicherheitsebene für die Anwender, da er eine Authentifizierung und Verschlüsselung der Datenübertragung unterstützt. OPC UA lässt sich nicht nur zur Kommunikation zwischen Automatisierungsgeräten verwenden, sondern liefert ebenfalls eine sichere und zuverlässige Methode zur Aktualisierung der Komponenten. Diese Funktion gibt dem Anwender die Gewissheit, dass seine Applikationen auf dem neusten Stand

der Technik sind respektive schnell und einfach upgedatet werden können.

Das in der Spezifikation OPC UA 10000-100 definierte Software-Aktualisierungsmodell wird zur Verwaltung der Software eines Assets eingesetzt. Dies kann die Installation neuer Software, Aktualisierung vorhandener Software, Aktualisierung einer Firmware sowie eine begrenzte Sicherung und Wiederherstellung von Parametern sowie der Firmware beinhalten, soweit es für die Aktualisierung erforderlich ist.

Betrieb als App oder Windows-Dienst

Der Standard OPC UA lässt sich unter anderem herstellerunabhängig für unterschiedliche Anwendungsfälle nutzen. Die Aktualisierung von Geräten kann über eine Client Software für das Update von Software – z.B. das Device and Update Management von Phoenix Contact – erfolgen. Um domänenspezifische Einschränkungen zu berücksichtigen, ist mit OPC UA auch eine domänenspezifische Client Software verwendbar. Diese hält dann bspw. in der Fertigungsdomäne einer Maschine vor der Aktualisierung an, während etwa in der Prozessdomäne ein redundantes Gerät aktiviert werden muss. Das Device and Update Management kann lokal an der Anlage als PLCnext App auf einem Industrie-PC von Phoenix Contact oder als Windows-Dienst auf einem PC mit Windows als Betriebssystem betrieben werden.

Grundsätzlich lässt sich die Software-Aktualisierung für jedes Gerät oder jede Softwarekomponente anwenden, die im Adressraum des Servers exponiert und über einen OPC UA Server erreichbar ist. Sollen in einer Maschine oder Anlage mehrere angeschlossene Geräte aktualisiert werden, unterstützt das Device- and Update-Management mit OPC UA ebenfalls dabei, wenn diese zunächst in einen speziellen Zustand zu versetzen sind, bevor die Aktualisierung startet. Auch die Reihenfolge der Updates auf den Geräten lässt sich dort einstellen, um für einen geordneten Update-Prozess zu sorgen.

Zur schnellen (Wieder-)Inbetriebnahme nach einem möglichen Systemausfall oder einem Gerätetausch wäre es sinnvoll, die Daten der Geräte regelmäßig zu sichern. An dieser Stelle erlaubt die Back-and-Restore-Funktion von OPC UA das Speichern der Daten. Die zuvor gesicherten Daten lassen sich ebenfalls auf das (neue) Gerät übertragen, sodass der ursprüngliche Zustand wiederhergestellt wird.

Integerer Bezug von Updates

Die Anlagenverantwortlichen oder Security-Teams müssen rechtzeitig über Updates der Asset-Hersteller informiert werden. Zu diesem Zweck setzt jeder Hersteller sein eigenes Verfahren zum Verteilen der Informationen sowie zum Aufspielen der Updates ein. Mit Manufacturing-X wird ein Lösungsansatz verfolgt, wie eine standardisierte und herstellerunabhängige Datenübertragung zwischen den Unternehmen funktioniert. Eine solche Vernetzung der kompletten Wertschöpfungskette bedingt jedoch gleichzeitig besondere Maßnahmen in puncto Datensicherheit. Mit den beschriebenen sowie umgesetzten und zertifizierten Maßnahmen zur Sicherstellung der Datensicherheit bietet das offene Ecosystem PLCnext Technology eine einzigartige Plattform, die optimal für die Manufacturing-X-Kommunikation vorbereitet ist. In Kombination mit der Nutzung von OPC UA und dem Device and Update Management lassen sich so Geräte-Updates direkt beim vom

© Phoenix Contact

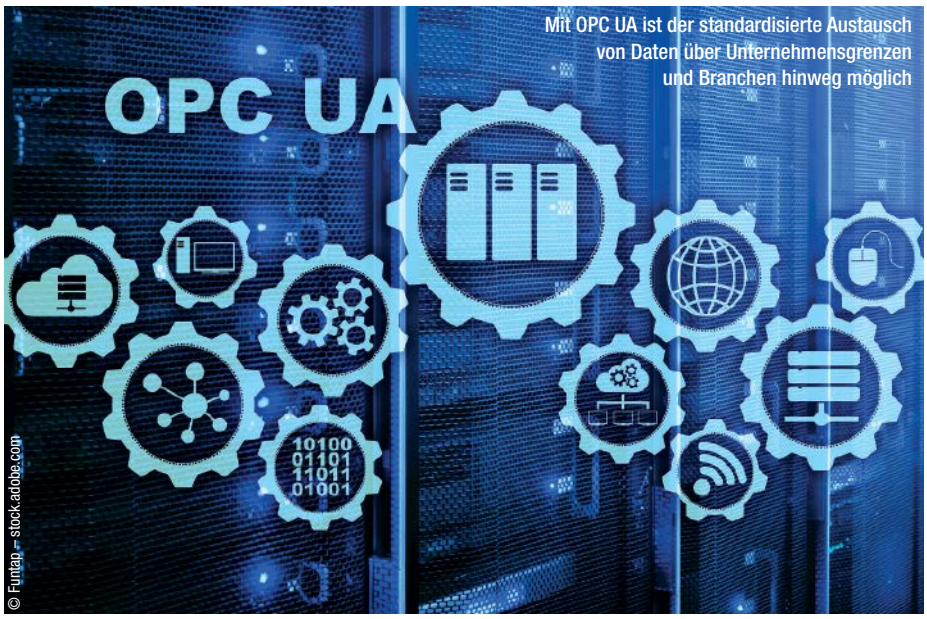
Redundanter Buskoppler für das Remote-I/O-System Axioline P

Mit der Produktfamilie Axioline P können Standard- und eigensichere (Ex i) Ein-/Ausgangssignale über redundante Modbus TCP-Buskoppler erfasst werden. In Ex-Zone 2 installiert, lassen sich die Signale der Ein-/Ausgangsmodule direkt aus den Ex-Zonen 0, 1 oder 2 anschließen. Die innovative Modbus-Redundanz in der Remote-I/O-Station erweitert die robuste Axioline P-Plattform um eine zusätzliche Funktion im Sinne der Hochverfügbarkeit. Das System kann mit zwei Buskopplern mit jeweils eigener IP-Adresse für die Client-/Server-Kommunikation unter Verwendung eines Redundanzmanagement-Funktionsbausteins konfiguriert werden. Die Buskoppler führen die Redundanzumschaltung intern in der Firmware durch und erfordern somit keine weitere Software. Bei einer Umschaltung des Buskopplers kommt es weder zu einem Datenverlust noch zu einer Unterbrechung der Datenübertragung mit der Steuerung.

Die Konfiguration der I/O-Station erfolgt einfach über einen integrierten Webserver. Alle angebundenen Axioline P-Ein-/Ausgangsmodule lassen sich ohne externe Software einstellen. Die hohe Verfügbarkeit des Systems wird neben der oben beschriebenen Funktion durch eine redundante Backplane und die Möglichkeit des Hot-Swapping von I/O-Modulen erreicht. In diesem Fall müssen die im laufenden Betrieb getauschten Ersatzmodule nicht konfiguriert werden.

© Phoenix Contact

Die Produktfamilie PLCnext Control hat vom TÜV Süd die OT-Security-Zertifizierung IEC 62443-4-2 erhalten; mit zunehmender Vernetzung und Digitalisierung von Anlagen und Produktionen erhöhen sich gleichzeitig auch die Anforderungen an ganzheitliche Sicherheitskonzepte



Mit OPC UA ist der standardisierte Austausch von Daten über Unternehmensgrenzen und Branchen hinweg möglich

© Funtap – stock.adobe.com

Arno Martin Fast,
Senior Specialist Digital Services, Phoenix Contact Electronics, Lemgo

Boris Waldeck,
Master Specialist Security PLCnext Technology and Product Solution Security Expert, Phoenix Contact Electronics, Bad Pyrmont

Wiley Online Library

Hersteller bereitgestellten Update Repository zyklisch im Hinblick auf neue Asset-Versionen erkennen. Ist ein Update verfügbar, kann es ohne Umwege integer bezogen und im Device and Update Management verwendet werden. Das Konzept der Industrie 4.0 erfordert eine einfach zugängliche, sichere und durchgängige Datenvernetzung über die gesamte Wertschöpfungskette. Mit PLCnext Technology und dem Device and Update Management liefert Phoenix Contact erste Anwendungen, die zeigen, was Manufacturing-X in Zukunft möglich macht.

Phoenix Contact GmbH & Co. KG, Blomberg
https://plcnext.help · www.phoenixcontact.de

Kompromittierungsschutz bei der Fernwartung

Mit der Unterstützung des offenen Internet Content Adaption Protocol (ICAP) ermöglicht der IT-Sicherheitsspezialist genua ab sofort die Anbindung weiterer externer Viren- und Malware-Scanner an seine Fernwartungslösung genubox. Mit dem zunehmenden Einsatz von Fernwartungszugängen in Produktionsumgebungen wird auch eine sichere Remote-Datenübertragung von Patches und Updates immer wichtiger. Um die Sicherheit operativer Technologie (OT) in kritischen Infrastrukturen und Industrieumgebungen zu gewährleisten und um eine Infektion von Geräten, Maschinen und Anlagen mit Firmware-Malware zu verhindern, ist es wichtig, die Integrität von Dateien vor dem Einspielen sicherzustellen. In der Vergangenheit wurde die Durchführung von Updates aus Sicherheitsgründen häufig durch den Einsatz physikalischer Medien oder spezieller elektronischer Datentransfers bewerkstelligt. Durch die Anbindung eines Viren- und Malware-Scanners via ICAP-Protokoll an die Fernwartungsumgebung kann dieser Schritt nun entfallen. ICAP ist ein offenes, leichtes Protokoll zur einfachen Weiterleitung von HTTP(S)- und FTP-Daten an einen ICAP-Server bzw. externen Virenscanner. Dieser Schritt verbessert den Schutz von Industrieanlagen vor Viren und Malware in Updates und Patches, die von Herstellern und externen Dienstleistern remote in ein Zielsystem eingespielt werden. Dabei hält die Rendezvous-Umgebung der Fernwartungslösung die zu übertragenden Dateien zunächst in einem standardmäßig angelegten Quarantäneverzeichnis zurück. Erst nachdem der über ICAP angebundene Malware-Scan-Server deren Überprüfung abgeschlossen und die Freigabe mittels HTTP-Code an die Servicebox gemeldet hat, werden die Daten an das Zielsystem übertragen. Dank der implementierten Logging-Funktionen können Fernwarter in regulierten Umgebungen die fehlerfreie Überprüfung und Übermittlung der Dateien in ihrem Audit-Trail nachweisen. In der Pharmaindustrie ist dies bspw. durch die „Good Manufacturing Practices“ (GMP) der Europäischen Arzneimittelagentur gefordert. Ähnliches gilt für Umgebungen, in denen ein Sicherheitsmonitoring notwendig ist. Hierzu verfügt die Servicebox über eine Schnittstelle zu SIEM-Systemen (Security Information and Event Management) zur zentralen Erfassung aller sicherheitsrelevanten Meldungen. Mit der Einbindung eines Malware-Scanners und der Nutzung des ICAP-Protokolls in der Rendezvous-Umgebung wurde das Sicherheitsniveau nochmals erhöht und der Einsatz einer weiteren Technologie für die Datenübertragung entfällt. Die Ausleitung von Daten über ICAP ist ab genubox Version 8.2 und höher möglich.

www.genua.de

Jetzt auch für den Außenbereich

Die modulare HMI-Plattform VisuNet FLX von Pepperl+Fuchs bietet besonders hohe Flexibilität. Ob Remote- oder Direktmonitor, Industrie- oder Box-PC: Die Baureihe umfasst verschiedene HMI-Systeme für unterschiedlichste Anwendungen und Montagesituationen in ATEX/IECEx-Zone 2/22, NEC 500 Div 2 und Non-Ex-Bereichen. Das modulare „One-Fits-All“-Design erlaubt die passgenaue Konfiguration von HMI-Lösungen und ermöglicht die einfache und schnelle Anpassung im Feld. Mit einer neuen Gehäusevariante wurde das Portfolio jetzt erweitert: Die Serie mit Aluminiumgehäuse ist in erweiterten Temperaturbereichen von -20 bis +50 °C und im Außenbereich einsetzbar. Das robuste Gehäuse leitet nicht nur Wärme effektiv ab, sondern ist auch hoch widerstandsfähig. Für eine gute Lesbarkeit auch bei sehr hellen Lichtverhältnissen verfügen die Geräte der Baureihe über ein optisch gebondetes Display. Nach Bedarf können zusätzlich Sonnenschutzelemente an den Seiten, der Oberkante und der Rückseite angebracht werden. Sie dienen gleichzeitig als Schutz vor Regen. Wie die Edelstahlvariante ist auch die neue Produktlinie mit Aluminiumgehäuse für den explosionsgefährdeten Bereich zugelassen (ATEX/IECEx-Zone 2/22 und NEC 500 Div. 2).

www.pepperl-fuchs.com