NOA, Ethernet APL und Cybersecurity

Mehr Daten aus der Produktion können Effizienz und Profitabilität steigern

Ethernet APL, die NAMUR Open Architecture (NOA) und Cybersecurity sind eng miteinander verbunden: sie zielen alle darauf ab, die Effizienz, Sicherheit und Datenverfügbarkeit in der Prozessindustrie zu verbessern. Ethernet APL stellt die physikalische Infrastruktur bereit, NOA ermöglicht die Nutzung zusätzlicher Daten, und Cybersecurity schützt diese Systeme vor Bedrohungen.


© Chatchanan - stock.adobe.com

Ethernet APL (Advanced Physical Layer) ermöglicht eine schnelle und zuverlässige Datenübertragung in der Prozessindustrie, selbst in explosionsgefährdeten Bereichen. Sie bietet eine einheitliche Ethernet-Kommunikation bis hin zur Feldebene und unterstützt Protokolle wie Profinet und OPC UA. Mit der zunehmenden Vernetzung durch Technologien wie Ethernet APL steigt auch die Notwendigkeit, diese Netzwerke vor Cyberangriffen zu schützen. Cybersecurity spielt eine zentrale Rolle, um die Integrität und Vertraulichkeit der übertragenen Daten zu gewährleisten. NOA schließlich erweitert die klassische Automatisierungsarchitektur, indem sie einen zweiten, sicheren Kommunikationskanal für zusätzliche Daten bereitstellt. Dieser Ansatz ermöglicht eine rückwirkungsfreie Übertragung von Produktionsdaten für Überwachung und Optimierung. Ethernet APL wird oft als physikalische Grundlage für NOA genutzt, da es die Datenübertragung bis zur Feldebene unterstützt. Neue Informationen zu diesen Themen gibt es aus den NAMUR-Arbeitskreisen.


© Anapur

> *Die Ethernet-Kommunikation bedingt größere Cyberrisiken und erfordert geeignete Sicherheitsmaßnahmen.*
>
> **Erwin Kruschitz, Anapur**

Ethernet APL – Security Advisory

Der NAMUR AK 4.18. Automation Security hat in einer Empfehlung die Realisierungsmöglichkeiten von Ethernet-APL-Installationen für Anlagen der Prozesschemie unter den Gesichtspunkten der IT/OT-Security beschrieben. Als Teil des weitverbreiteten Ethernet-Standards bietet Ethernet APL ein hohes Maß an Robustheit für einen zuverlässigen Betrieb und ermöglicht Chancen bei Anwendungen, die höhere Ansprüche an Datenmenge und Durchsatz haben. Dazu gehören:

- bessere Analysemöglichkeiten durch höhere Bandbreite
- Zugriffsverfolgung und Nachverfolgung
- Rollen- und Rechtemanagement
- Änderungsmanagement
- Assetmanagement-Anbindung an zentraler Stelle.

Die technologischen Unterschiede zwischen APL und traditioneller Anlagen-Kommunikation (TAK) mit 4-20 mA-Anbindung ohne und mit zusätzlicher HART-Kommunikation oder Feldbussen (Profibus PA, Foundation Fieldbus) macht jedoch auch die Durchführung einer zusätzlichen IT/OT Risikoanalyse notwendig.

Aus der IT-Security-Perspektive gibt es mehrere Gründe, warum im Vergleich zur TAK zusätzliche Risiken mit Ethernet-APL verbunden sind, z.B.:

- Vergrößerte Angriffsfläche: Ethernet-APL ist eine digitale Kommunikationsschnittstelle, mit der Standard-Ethernet/IP-basierte Netzwerke errichtet werden. Diese stärkere Vernetzung über etablierte Protokolle stellt eine zusätzliche Angriffsoberfläche dar und eröffnet Möglichkeiten für Cyberangriffe, wie Spoofing von Daten, Denial-of-Service-Angriffe, Malware und andere digitale Bedrohungen, die bei TAK nicht vorhanden sind.
- Netzwerkverbindungen: Ethernet-APL-Komponenten bilden Netzwerke, d.h. sie sind potenziell anfällig für netzwerkbasierte Angriffe. Angreifer könnten versuchen, in das Netzwerk einzudringen, um auf kritische Systeme und Daten zuzugreifen.
- Komplexität der Systeme: Digitale Systeme sind oft komplexer als analoge Systeme, was bedeutet, dass sie mehr potenzielle Schwachstellen aufweisen. Die Vielzahl an Komponenten, Protokollen und Software kann zu Fehlkonfigurationen führen, die potenzielle Sicherheitsrisiken darstellen oder es aufwendiger machen Schwachstellen zu finden.

APL bietet also aus der IT-Security-Perspektive mehrere Risiken, die in der TAK nicht oder weniger ausgeprägt vorhanden sind. Erwin Kruschitz, CEO Anapur und Leiter des NAMUR AK 4.18, betont: „Die stärkere Vernetzung unter Verwendung von Standard-Ethernet/IP-Kommunikation und die dadurch bedingte größere Angriffsfläche macht es wichtig, geeignete Sicherheitsmaßnahmen zu implementieren, um diese Risiken zu minimieren." Dazu gehören

- Physische Sicherheit (Betreiber)
- Netzwerksegmentierung (Betreiber)
- Schwachstellenmanagement (Betreiber/Hersteller)
- Updatefähigkeit der Geräte über den gesamten Lebenszyklus (Betreiber/Hersteller)
- Geräte müssen die Integrität der gespeicherten Daten gewährleisten (Hersteller)
- Logischer Zugriffsschutz und Härtung (Betreiber/Hersteller)
- Erfassung von Systemzugriffen und -änderungen (Betreiber/Hersteller).

Härtung von Computersystemen

Ein weiteres Papier des NAMUR AK 4.18 zielt auf die Härtung von Automatisierungssystemen. Unter dem Begriff Härten (englisch Hardening) versteht man die Entfernung aller Softwarebestandteile und (Hardware-) Funktionen, die zur Erfüllung einer vorgesehenen Aufgabe durch das Programm oder System nicht zwingend notwendig sind – Systemhärtung zielt also darauf ab, die Angriffsfläche eines Systems zu verkleinern. Auch durch die aktive Nutzung von Benutzerkontensteuerungen, Logging (also die automatische Erstellung eines Protokolls von Ereignissen wie Fehler- oder Statusmeldungen während des Betriebs eines IT-Systems) und Berechtigungsmanagement kann eine zusätzliche Härtung erreicht werden.

> *Ethernet APL bietet ein hohes Maß an Robustheit für einen zuverlässigen Betrieb und ermöglicht Anwendungen, die höhere Datenanforderungen haben.*

Im Hinblick darauf, dass alle Systeme der Automatisierungstechnik direktes Ziel eines Angriffs sein können, werden die klassischen Sicherheitsziele Vertraulichkeit (C = Confidentiality), Integrität (I = Integrity) und Verfügbarkeit (A = Authenticity) grundsätzlich erstmal alle berührt.

- C: Möchte der Angreifer Informationen ausspähen, verhindert ein gehärtetes System dies nicht, kann aber den Zugriff auf diese erheblich erschweren. Somit stellt ein gehärtetes Zielsystem (z.B. Leitsystemserver, Controller) ggf. zusammen mit gehärteten Schutz-Systemen (z.B. Firewall, Quarantänerechner) einen Grundbaustein für die Sicherheit von Informationen dar.
- I: Bei der Integrität von Systemen spielt im Zusammenhang mit Härtung der Punkt „Korrektheit von Software" eine wichtige Rolle. Programmlücken oder Programmierfehler in einer einzelnen Softwarekomponenten können die Integrität des gesamten Systems gefährden. Da die Härtung eines Systems, die Entfernung nicht benötigter Software und Komponenten einschließt, kann Härtung also die Integrität erhöhen.
- A: Ein System, das durch Härtung schwerer zu attackieren ist, ist grundsätzlich höher verfügbar. Ein positiver Nebeneffekt der geringeren Komplexität ist, dass das Auftreten von Fehlern bei der Ausführung von Programmen unwahrscheinlicher wird. Auch das steigert die Verfügbarkeit.

Gängige Betriebssysteme besitzen standardmäßig keine sehr restriktive Sicherheitskonfiguration und sind potenziell mit ungenutzten Komponenten ausgestattet, die häufig als Einfallstor von Angreifern missbraucht werden. Ein gehärtetes System stellt nur die Funktionen bereit, die für die Erfüllung seiner Aufgabe unbedingt erforderlich sind. Als Nebeneffekt reduziert dies ebenfalls den Aufwand für die Pflege und Aktualisierung der betroffenen Systeme.

Wichtige Komponenten der Netzwerk-Infrastruktur in Automatisierungssystemen stellen Switche, Router oder Firewalls dar. Bei der Konfiguration dieser Geräte sollte man unbedingt die ab Werk eingerichteten Standard-Passwörter ändern. Außerdem sollten, wenn möglich, schwache bzw. veraltete Protokolle wie Telnet, SMB V1.0 – 3.0 oder SNMP 1.1 – 2 ausgeschaltet sowie nicht benutzte LAN-Ports ebenfalls deaktiviert werden.

Mobile Geräte wie Smartphones und Tablets spielen auch in der Prozessautomatisierung eine immer größere Rolle. Wie Wechselmedien bringen aber auch sie die potenzielle Gefahr mit sich, Schadcode bei Verbindung zu einem (Automatisierungs-) System zu übertragen oder andere ungewollte Einflüsse zu haben. Grundsätzlich gilt die Empfehlung, mobile Geräte hinsichtlich Härtung genau wie die bereits genannten Systeme auch zu behandeln.

NE178 NAMUR Open Architecture: Verification of Request

Das Ausnutzen moderner IT-Technologien in Kombination mit bewährten und sicheren OT-Architekturen ist unerlässlich, um marktwirtschaftliche Vorteile zu erkennen und zu nutzen. Dafür muss grundsätzlich Information zwischen den IT/OT-Bereichen sicher ausgetauscht werden.

Ziel des in NE 175 ausgeführten Konzepts der NAMUR Open Architecture (NOA) ist es, innovative und effiziente Standard-IT-Technologien in der industriellen Prozessautomatisierung einzusetzen. NOA beschreibt eine additive Architektur, um Informationen zwischen den drei Bereichen OT/Kernautomatisierung (CPC), plant specific optimization (psM+O) und central monitoring and optimization (M+O) auszutauschen. Durch die Verwendung offener Informationsmodelle (NE176), Aggregations-Servern (NE179) und Sicherheits-Gateways (NE177) macht NOA CPC-Informationen für eine Vielzahl von Anwendungen im Bereich psM+O und M+O zugänglich. Mit NOA Verification of Request (VoR) wird ein weiteres Puzzlestück in NOA gelegt: Es beschreibt, wie Informationen (Handlungsempfehlungen) aus dem „äußeren" psM+O hochautomatisiert zurück in OT/CPC kommunizieren werden können, ohne die Verfügbarkeit oder Sicherheit der Anlage zu gefährden.

Die aktuelle NAMUR-Empfehlung NE178/VoR

- beschreibt eine zwischen psM+O und CPC verteilte System-of-Systems-Architektur
- beschreibt eine Reihe notwendigen, sequenziellen Informationsverarbeitungsschritte. (Authentifikation & Authorisierung, Verifikation, Abbildung, Annahme und Abbildungsverifikation), die angewendet werden müssen, damit Informationen sicher und zuverlässig zwischen den IT/OT-Bereichen kommuniziert werden können
- schützt das Know-how über die interne Architektur und spezifische Automatisierung einer Anlage
- beschreibt einen Rückmeldungsmechanismus, der dem Aussteller einer Anfrage über den Verarbeitungsstatus informiert ohne Anlageninterna preis zu geben
- enthält detaillierte Empfehlungen für die Administration und das Betreiben von VoR-Systemen
- führt beispielhaft vereinfachte Anwendungsbeispiele auf.

Wichtiges Ziel von VoR ist es, die Integrität, funktionale Sicherheit, Verfügbarkeit und IT-Sicherheit der CPC-Domäne mit allen erforderlichen Mitteln zu erhalten, während Informationen Domänengrenzen genau definiert, steuerbar, wiederholbar, automatisiert und nachvollziehbar überschreiten.

Fazit

Künstliche Intelligenz wird heute schon in vielen Bereichen eingesetzt. Wenn KI helfen soll, auch die operationellen Bereiche der Prozessindustrie von Upstream bis Downstream durchgängig zu optimieren, sind belastbare Daten aus der Produktion zum Trainieren der KI unerlässlich. Ethernet APL und NOA bieten die Grundlagen, diese Daten zur Verfügung zu stellen. Die notwendigen Cybersecurity-Maßnahmen müssen einen ungefährdeten Datentransfer sicherstellen.

Volker Oestreich, CHEManager

- www.namur.de