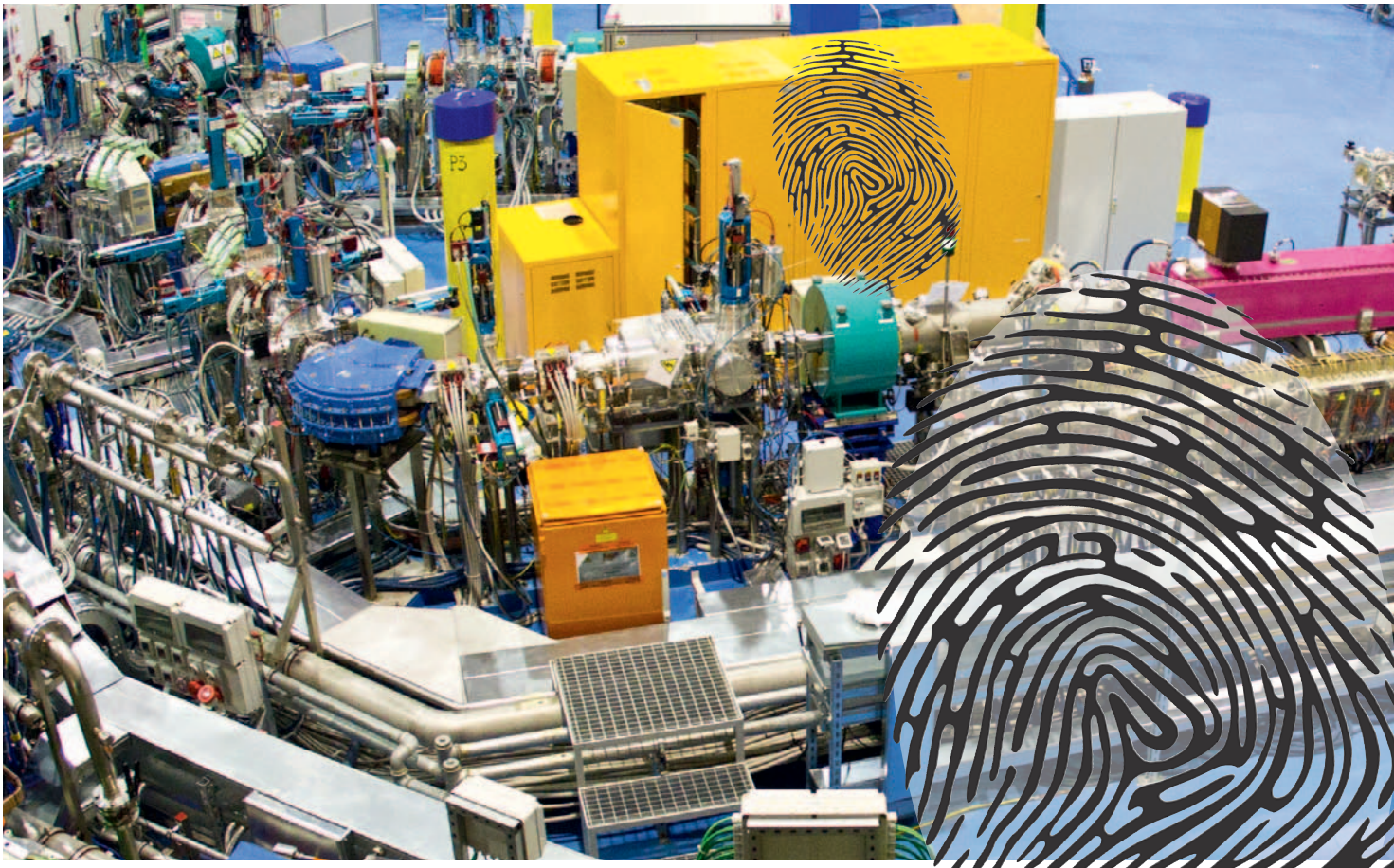


Bildquelle: National Instruments; Chepe/Fotolia.com

Auf die Schnelle

Das Wesentliche in 20 Sek.

- Sicherheitskonzepte aus der IT eignen sich nicht zwangsläufig für die Automatisierung
- denn gängige IT-Sicherheitsmaßnahmen behindern das Hauptziel der Automatisierungstechnik: die Verfügbarkeit des Netzwerks
- eine permanente Netzwerküberwachung hilft, Angreifer im Netzwerk zu erkennen

später lesen/ weiter empfehlen

IT-Security als Blaupause ungeeignet

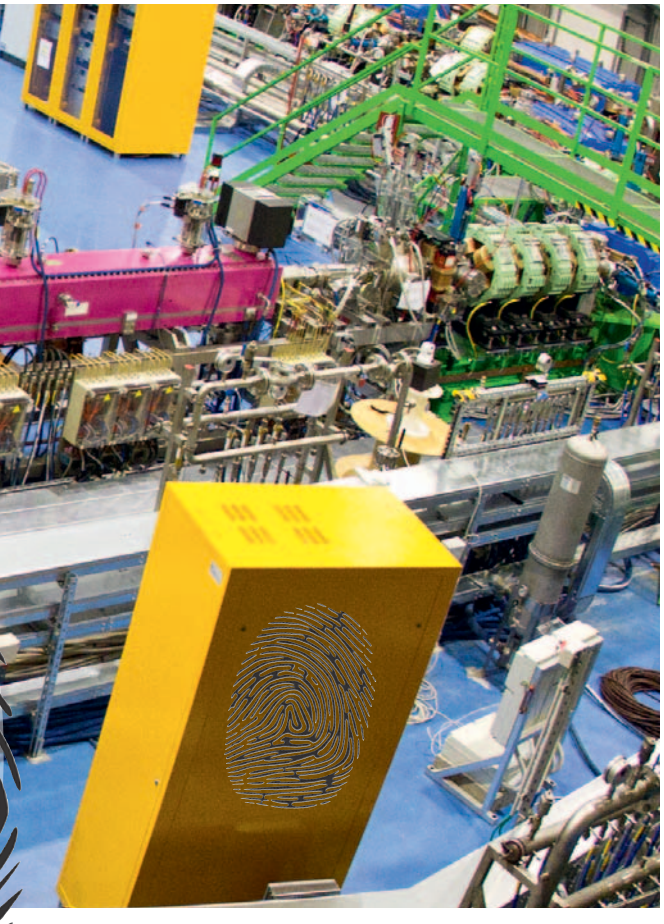
Automatisierung 4.0

Die Verschmelzung von Maschinen- und Produktionsnetzwerken im Zuge von Industrie 4.0 erfordert moderne Security-Konzepte, die neben dem Schutz auch die Maschinen- und Anlagenfunktion erhalten. Nun lädt die immer stärkere Verzahnung der Automatisierungstechnik mit der IT förmlich dazu ein, deren Sicherheitskonzepte schablonengleich zu übernehmen. Jedoch sind die Maßnahmen, die die IT bereitstellt, für die Automatisierung ungeeignet.

Autor: Christian Wiesel

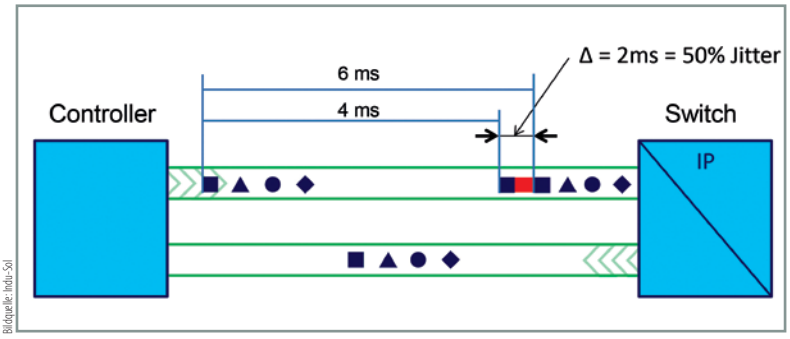
Die als Security-Instanzen in der IT etablierten Router und Firewalls sind für automatisierte Netzwerke überflüssig. Denn die Verbindungsstelle zwischen Büro- und Produktionsnetzwerk ist entweder bereits durch die IT-Abteilung des Unternehmens abgesichert oder die Maschinen sind erst gar nicht in das Büronetzwerk eingebunden. Eine weitere Sicherheitsmaßnahme aus der IT ist der Einsatz aktiver Scantools: Diese identifizieren unberechtigte Teilnehmer im Netzwerk und ermitteln das Benutzerverhalten sowie den Ressourcenverbrauch, produzieren jedoch zusätzlichen Traffic. Damit erhöhen sie die Netzlast und behindern den wesentlichen Datenverkehr, der für eine reibungslose Maschinen- und Anlagenfunktion notwendig ist. Auch die Verschlüsselungsverfahren der IT scheiden für die Automatisierer als Maßnahme aus, da Codierung und Decodierung den Anforderungen an Echtzeitkommunikation moderner Netzwerke zuwider laufen.

Wer trotz stumpfer Waffen seine Festung schützen will, könnte immerhin einen Grenzzaun ziehen. Praktisch heißt das in der IT, den sogenannten Backbone – die Hauptverkehrsader des Datenstromes – vor unbefugtem Zugriff auf die Daten abzuriegeln. Wür-



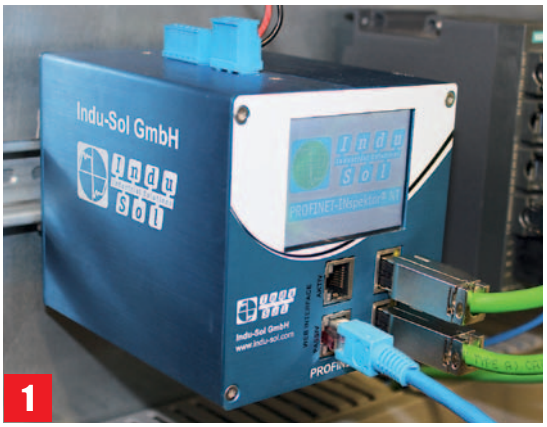
In der Automatisierungstechnik können Angriffe von innen und außen derzeit nicht verhindert werden. Jeder Angreifer hinterlässt jedoch Spuren – permanente Überwachungslösungen warnen die Betroffenen.

den Automatisierer dies in ihren Netzwerken tun, hätten allerdings auch die Mitarbeiter sowie Partner keinen Zugriff mehr. In den Anlagen müssen jedoch Zugangspunkte zum Netzwerk bestehen, da sie für Programmierung, Diagnose oder andere Servicedienstleistungen durch Mitarbeiter oder externe Auftragnehmer essenziell sind. Speziell im Fehlerfall, wenn akut Gegenmaßnahmen zum Erhalt der Maschinen- und Anlagenfunktion zu ergreifen sind, schmerzt jede Sekunde Zeitverlust, der durch Zugangsprobleme verursacht wird und am Ende durch einen Produktionsausfall Geld kostet. Die gängigen Security-Maßnahmen aus der IT behindern also das Hauptziel der Automatisierungstechnik, nämlich die Verfügbarkeit des Netzwerks und damit die Anlagenfunktion hoch zu halten. Daher muss die Automation eigene Wege gehen.



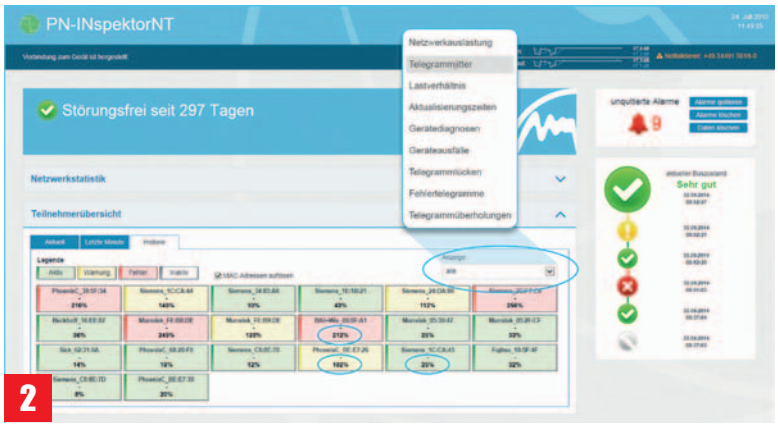
Bildquelle: Indu-Sol

Eine verzögerte Ankunft von Telegrammen (Jitter) kann ein Hinweis auf einen ungebetenen Netzwerkteilnehmer sein.



Bildquelle: Indu-Sol

1



Bildquelle: Indu-Sol

2

[1] Der Profinet-Inspektor NT analysiert permanent den logischen Datenverkehr und warnt den Betreiber sofort bei Auffälligkeiten.

[2] Auf der Weboberfläche des Profinet-Inspektors NT werden die Analyseergebnisse sofort angezeigt – ohne zusätzliche Software. Die Chronik rechts zeigt den aktuellen Zustand des gesamten Busses. Der ermittelte Jitter wird teilnehmerbezogen entsprechend der Höhe der Abweichung nach dem Ampelprinzip farblich unterlegt.

Anomalien erkennen – die Alternativen

Wer nicht von Funktionsstörungen oder Anlagenstillständen überrascht werden will, setzt bei seinen Anlagen auf eine permanente Netzwerküberwachung (PNÜ). Diese Lösungen sind in der Lage, eine sogenannte Plausibilitätserkennung durchzuführen. Sie analysieren, ob Telegramme bestimmte Vorgaben wie Zeit und Inhalt einhalten. Abweichungen werden sofort erkannt und gemeldet. Somit können Anwender eine große Bandbreite an Szenarien detektieren: von vergleichsweise banalen Zwischenfällen wie das unbedachte Aufstecken eines Laptops auf die Anlage durch einen Mitarbeiter bis hin zu technisch ausgefeilten Angriffen wie Cyber-Attacken. Der Grund: Durch das Zwischenschalten des Angreifers entsteht ein zeitlicher Verzug bei der Datenübertragung, der sogenannte Jitter. Informationen lassen sich dadurch nicht in der vorgegebenen Zeit verarbeiten (Aktualisierungsrate). Von außen und ohne permanente Überwachungslösung ist diese Verspätung nicht zu erkennen. Ist der Angreifer erst einmal im Netzwerk, hat der Betroffene seine Chance verpasst, ihn auf frischer Tat zu ertappen. Im Gegensatz zur IT, wo selbst moderne Sicherheitssysteme getarnte Angriffe mitunter kaum erkennen können, hinterlässt ein unbekannter Teilnehmer im Netzwerk einer automatisierten Anlage jedoch garantiert Spuren. Indem diese Anomalien aufgezeichnet und die zugehörigen Daten archiviert werden, erhält der Betreiber wichtige sicherheitsrelevante Hinweise und damit eine reelle Chance, den Angriff zu erkennen sowie notwendige Gegenmaßnahmen einzuleiten.

Unerwünschte Teilnehmer erkennen

Während Sicherheitssysteme in der IT eine Selbstverständlichkeit sind, bleiben aufseiten der Automatisierungstechnik die Aktivitäten hinsichtlich der Weiterentwicklung des Security-Bereiches bislang überschaubar. Erste Unternehmen reagieren mit umfassenden Sicherheitsrichtlinien. Dies ist jedoch mit Nachteilen verbunden: Wird beispielsweise ein externer Dienstleister gerufen, um die Anlagenverfügbarkeit wiederherzustellen und einen (möglichen) Schaden eines (anstehenden) Produktionsausfalls gering zu halten, muss er sich zuerst in das Regelwerk von Security-Anweisungen einlesen.

Die geforderten Funktionalitäten lassen sich dagegen in einem Produkt vereinen: Der Profinet-Inspektor NT von Indu-Sol beispielsweise ist ein intelligentes, permanentes und passiv arbeitendes Mess- und Diagnosetool für Profinet-Netzwerke. Es überwacht den logischen Datenverkehr und speichert Ereignisse wie Jitter, Telegrammfehler beziehungsweise fehlende Telegramme oder Geräteausfälle. Bei Veränderungen und somit Überschreitung voreingestellter Schwellwerte der Qualitätsparameter im Netz werden Alarmmeldungen über verschiedene Kanäle wie SNMP, E-Mail oder die Weboberfläche des Inspektors abgesetzt. Bisher passiert all dies primär mit dem Fokus auf der Netzwerkverfügbarkeit. Das Gerät und die Vorgehensweise eignen sich jedoch ebenso dazu, dem Anwender sicherheitstechnische Hinweise zu liefern. Denn er kann historische Ereignisse nachvollziehen und erhält Hinweise auf Teilnehmer, die sich im laufenden Betrieb ins Netzwerk eingeschaltet haben – eben auch unerwünschte. Sollte der Elektroinstandhalter nicht in der Lage sein, die automatisch aufgezeichnete Anomalie auszuwerten, lässt sich der Telegrammmitschnitt einem Fachmann übermitteln.

Will die Automatisierungstechnik das volle Potenzial der Industrie 4.0 ausschöpfen, muss sie ihre Netzwerke mit zeitgemäßen Security-Systemen ausrüsten. Wie beschrieben sind die aus der IT bekannten Maßnahmen als Vorlage ungeeignet. Da sich jedoch mittlerweile Lösungen zur permanenten Netzwerküberwachung etabliert haben, können diese mitgenutzt werden, um erste Schritte in Richtung eines modernen Security-Systems zu gehen. *(mns)*

Autor
Christian Wiesel
ist tätig im Marketing der Indu-Sol GmbH in Schmölln.