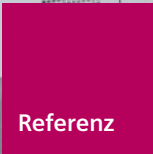




SIEMENS



Referenz

Höchstmaß an Sicherheit im Produktionsnetzwerk

Zellensegmentierung von Produktions-
anlagen sowie gesicherter Internet- und
Intranetzugriff dank Managementplattform
für Remote Networks

Für die Fertigungsautomation hat die Festo AG in ihrer Technologiefabrik Scharnhausen eine neue Sicherheitsplattform eingerichtet. Funktionen wie Firewall und VPN-Verschlüsselung bieten erhöhten Schutz bei der Datenübertragung und schotten die Produktionsnetze gegen ungewollte Zugriffe von außen und innen ab. Dies steigert die Prozesssicherheit und erhöht die Produktivität der gesamten Fertigungsumgebung.

Die Festo AG ist ein Global Player im Bereich der pneumatischen und elektrischen Automatisierungstechnik. Das Unternehmen mit Sitz in Esslingen am Neckar liefert etwa 33.000 Katalogprodukte und einbaufertige Automatisierungssysteme an seine Kunden weltweit. Jährlich werden etwa 15.000 maßgeschneiderte Lösungen entwickelt und produziert. Neben der Automatisierungstechnik steht bei Festo die Digitalisierung im Mittelpunkt der Betrachtung. Diese beschränkt sich nicht nur auf intelligente Produkte, sondern umfasst die gesamte Wertschöpfungskette von der Planungsphase über Komponenten und Systeme bis hin zur Produktion und vorausschauenden Instandhaltung. Hier spielt vor allem die Hard- und Software eine wichtige Rolle, um die Fertigungssysteme sicher miteinander zu vernetzen und damit Industrie 4.0 zu ermöglichen.

„Die Digitalisierung der industriellen Automatisierungssysteme ist verbunden mit zunehmender Vernetzung, großen Datenmengen und der Verwendung offener Standards, mit der Durchgängigkeit erreicht wird“, beschreibt Albrecht Salm, Chief Information Security Officer bei der Festo AG. „Die Schattenseite dieser Entwicklung ist die Verwundbarkeit der Systeme gegenüber Cyberangriffen. Die Netzwerke im Produktionsbereich sind zu Angriffszielen geworden; das Vorgehen der Angreifer wird zunehmend aggressiver.“



„Wir haben eine Lösung realisiert, mit der ein sicherer Remote-Zugriff auf Maschinen und Fertigungsanlagen gewährleistet ist.“

Albrecht Salm,
Chief Information Security
Officer bei der Festo AG.

Mit Industrial Remote Access hat die Festo AG ihre Vorstellung einer gesicherten, vernetzten Produktionsumgebung umgesetzt. Salm weiter: „Mitarbeiter der Bereiche Global-IT und Instandhaltung haben eine Lösung realisiert, mit der nicht nur Maschinen und Fertigungsanlagen inklusive deren Applikationen miteinander kommunizieren, sondern auch der gesicherte Internet- und Intranet-Zugriff zum Beispiel auf die Speicherprogrammierbare Steuerung (SPS) der Maschinen gewährleistet ist.“

Eine große Herausforderung für die Werksinstandhaltung sind auch die unterschiedlichsten Netzwerkkomponenten und Router der Anlagen, die nicht „patchbar“ sind und sich für Festo als eine unsichere „Black Box“ darstellen.

„Die neue Managementplattform für die Produktionsnetzwerke hat unsere Erwartungen voll erfüllt. Neben dem integrierten Berechtigungsmanagement können Key-Plug und Ports der Router einfach und effizient konfiguriert werden.“

Lucia Tandjung,
Projektleiterin der Festo
Global IT



Zuverlässige Abläufe im gesamten Fertigungsnetz

„Wir hatten im Bereich Operational Technology (OT) einen Punkt erreicht, wo es darum ging, die Produktionsnetze sicherer und zentral administrierbar zu machen“, erläutert Lucia Tandjung, Projektleiterin der Festo Global-IT.

„Bis zu diesem Zeitpunkt gab es keinen einheitlichen Fernzugriffsstandard. Erklärtes Ziel war, den Zugriff externer und interner Servicemitarbeiter auf die Werkzeugmaschinen deutlich einzuschränken. Produktionsnetze bilden das Rückgrat unserer Automatisierungsumgebungen. Wenn ein externer Techniker mit seinem Service-Notebook unbeabsichtigt einen Virus ins Netz einschleust, gäbe es unter Umständen einen „Flächenbrand“ und der Anlagenverbund des gesamten Werks würde lahmgelegt“, gibt die Festo-Projektleiterin zu bedenken.

„Schon vor Projektstart waren Office- und Produktionsnetze voneinander getrennt, sodass der Zugang aus der Produktionsumgebung ins Office-Netzwerk nicht ohne weiteres möglich war. Mit dem Aufbau der neuen Technologiefabrik wurde zudem die Segmentierung der Produktionsnetze angegangen“, beschreibt Matthias Hieber, Projektleiter der Festo-Instandhaltung und verantwortlich für die Anlagenanbindung.

„Das Leistungsportfolio der Automatisierungskomponenten und des Engineering-Frameworks bietet die Möglichkeit, unsere Aufgabenstellungen optimal zu lösen.“

Matthias Hieber,
Projektleiter der Festo-
Instandhaltung und
verantwortlich für die
Anlagenanbindung.



„Im Rahmen eines Sicherheitsaudits der bisher eingesetzten Fernwartungslösungen stellte sich jedoch heraus, dass die Trennung beider Netzwerke den hohen Sicherheitsanforderungen alleine nicht gerecht wurde.“

Daher plante das Projekt-Team zeitgleich eine weitere Feinsegmentierung, um auch einzelne Fertigungsanlagen oder einzelne Legacy-Komponenten komplett abzuschotten.

„Die erhöhten Sicherheitsanforderungen verlangten einen gemanagten Zugriffspunkt, der durch die Instandhaltung mit internen und externen User-Rechten gepflegt wird und nicht durch eine Vielzahl verschiedener Gateways, deren Zugriffsrechte teilweise unbekannt sind“, schildert Hieber.



Für die Herstellung von Präzisionsbauteilen setzt Festo Fertigungsinseln ein. Über SCALANCE S615 sind die Maschinen in das Produktionsnetzwerk eingebunden und gegen unbefugte Zugriffe geschützt.

Hersteller haben individuelle Fernwartungslösungen für ihre Werkzeugmaschinen und richten Anlagenteile als Netzwerkkomponenten ein, was Wartungsarbeiten immer komplexer macht. Instandhaltungs-Experte Hieber weiter: „Bis zur Einführung der neuen Sicherheitsplattform konnten sich die Maschinen eigenständig mit dem Internet verbinden. Hersteller rüsteten ihre Anlagen mit Mobilfunk-Modems aus, über die sie zum Beispiel anhand von Grenzwerten Alarmmeldungen per SMS oder E-Mail versandten. Aber auch für jede Anpassung wählten sich die Maschinenhersteller direkt in das Festo-Netzwerk ein. Unsere Instandhalter konnten nicht remote auf interne Anlagenkomponenten zugreifen und mussten sich teilweise für SPS-Programmänderungen und Statusabfragen zunächst beim Hersteller einloggen. Von dort ging die Verbindung zurück auf die jeweilige Maschine im Werk.“ Dieses Verfahren war sehr unsicher und veranlasste das Projekt-Team dazu, Hersteller zur Neuordnung der IP-Adressen ihrer Maschinen gemäß Festo-Vorgaben aufzufordern. Diese Lösung war aber in den meisten Fällen nicht umsetzbar. Außerdem konnte das Ändern von IP-Adressen zum Gewährleistungsverlust der Anlagen führen.

Beseitigung von IP-Adresskonflikten, Segmentierung der Profinet-Teilnehmer

„Die Einführung der Siemens-Lösung hat die IP-Adresskonflikte beseitigt“, betont Lucia Tandjung. „Der Einsatz der Managementplattform SINEMA Remote Connect bietet uns, aber auch den Lieferanten der Maschinen, den Vorteil, dass sie ihre IP-Adressen nicht mehr modifizieren müssen. Sämtliche Anlagenzugriffe laufen nur noch über SINEMA Remote Connect mit einer zentralen IP-Adresse für den Zugang von außen.“ Die neue Server-Applikation nimmt sämtliche Tunnelverbindungen (VPN) an und vermittelt so zwischen den Client-PCs der externen Servicetechniker und den Maschinen. Die Kommunikation ist dabei protokollunabhängig, herstellernerutral und IP-basiert. Ein direkter und unkoordinierter Zugriff auf die Produktionsnetzwerke wird vermieden.

Mit SINEMA RC Client ist zudem eine Adressbuchfunktion verfügbar, über die sich Maschinen und Anlagen in der Technologiefabrik eindeutig identifizieren und für den gesicherten Wartungszugriff auswählen lassen. Die Maschinen werden vom Anlagenbauer mit unveränderten IP-Adressen installiert und über die Security Appliance SCALANCE S615 mit dem Netzwerk verbunden. SCALANCE S615 übernimmt auch die Übersetzung der IP-Adressen (Network Address Translation, kurz NAT), damit sich zwei verschiedene Netzwerke (intern und extern) über eine Firewall miteinander verbinden lassen.

Die Maschinen in der Fertigung sind nicht direkt von außen erreichbar, da sie durch NAT inklusive Firewall versteckt sind. Eingehende Datenpakete, die von einem externen Netz kommen und an eine externe IP-Adresse der Maschine (Ziel-IP-Adresse) gerichtet sind, werden in SCALANCE S615 durch die interne IP-Adresse ersetzt. Nur wenige Profinet-Zellenteilnehmer dürfen mit dem Festo-Office-Netz bzw. Applikationen über IP kommunizieren. Auch der frühzeitige und teilweise notwendige Remote-Zugriff auf Neuanlagen, die sich noch in der Fertigungsphase beim OEM befinden, kann mit den Security Appliances realisiert werden.

Als erstes rüsteten die Festo-Instandhalter eine Produktionslinie zur Ventilverfertigung mit SINEMA Remote Connect aus. Die Produktionslinie umfasst eine CNC-Rundtakt-Transfermaschine für das Bohren und Drehen der Werkstücke, eine Maschine für Hochdruck-Entgraten, einen Handling-Roboter und ein System für die Zu- und Abfuhr der fertigen Werkstücke. Die einzelnen Stationen sind mit den Ports der SCALANCE S Security Appliance verbunden. Die Security Appliance kommuniziert über einen verschlüsselten VPN-Tunnel mit der Managementplattform. Am SCALANCE S kann im Servicefall über einen Schlüsselschalter der VPN-Tunnel aktiviert werden, oder der Remote User wird auf der Managementplattform SINEMA Remote Connect temporär aktiviert. Ähnlich einem USB-Stick, aber ohne die Gefahr, Viren einzuschleusen, speichert ein Key-Plug sämtliche Konfigurationsdaten der Security Appliances, was einen schnellen und unkomplizierten Gerätetausch während des Produktionsbetriebs möglich macht.



Die Security Appliance SCALANCE S615, die Steuerung SIMATIC S7-1500 sowie die Stromversorgung SITOP PSU8200 sind bei Festo im Schaltschrank eingebaute Komponenten.

Bei der Kombination der Maschinensteuerungen SIMATIC S7-1500 und der HMI-Panels aus dem SIMATIC-Portfolio mit dem Engineering-Framework TIA Portal stand die hohe Effizienz und Flexibilität der Lösung im Vordergrund der Entscheidung. Nach extern werden nur Bildschirm- und Tastatordaten eines Festo-Instandhalters übertragen, denn der Zugriff auf die Anlagenzelle erfolgt für externe User nur über einen virtuellen Jump Host-Rechner, wo auch z. B. das TIA Portal als Floating-Lizenz zur Parametrierung der Anlagen zur Verfügung gestellt wird. Die Remote Session wird auch zur Revisionssicherheit auf Video aufgezeichnet, und die Projekte werden auf einem Festo-Backup-Server zentral gesichert. Ein externes Field PG bzw. Notebook ist durch dieses zweistufige Fernwartungskonzept von dem Festo-Netzwerk entkoppelt.

Festo-Projektleiter Hieber: „Das Leistungsportfolio der Automatisierungskomponenten und des Engineering Frameworks bietet die Möglichkeit, unsere Aufgabenstellungen optimal zu lösen. Durch die einfache Handhabung kommen wir sehr schnell zu den gewünschten Ergebnissen“, so der Technische Projektleiter und OT-Spezialist.

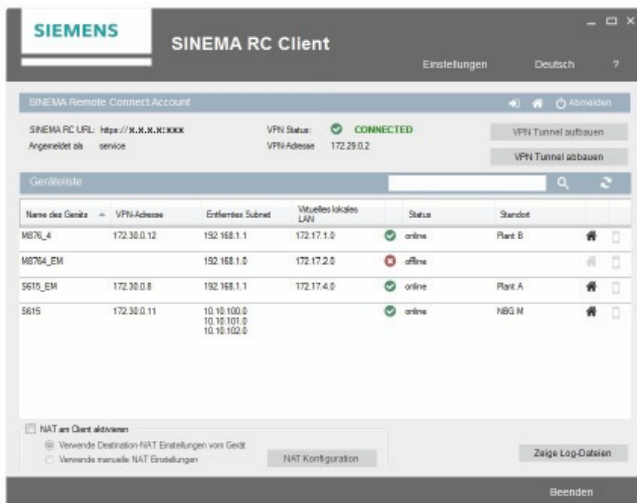
Festo Didactic-Trainings mit SINEMA Remote Connect und SCALANCE-Switches

Parallel zur Einführung dieser Fernwartungslösung in der Fertigung bietet die Festo Didactic SE basierend auf den eingesetzten Produkten SINEMA Remote Connect und SCALANCE S615 sowie weiterer Komponenten wie managed Switches der SCALANCE X-Familie ein Schulungsprogramm für Festo-Mitarbeiter an. Den Angestellten aus der Instandhaltung und angrenzenden Berufsfeldern werden dabei Netzwerk- und IT-Security-Inhalte vermittelt, die zum Verständnis und zum Betrieb der eingesetzten Lösung benötigt werden. „Um Festo-Mitarbeitern die sicherheitsrelevanten Aspekte der Fertigungsumgebung näherzubringen, haben wir das Training am Beispiel des Einsatzes von SINEMA Remote Connect und SCALANCE entwickelt“, beschreibt Dr. Matthias Kabatnik, zuständig für IT-Security-Lösungen im Global Solution Center bei Festo Didactic.

„Wir informieren über die Notwendigkeit, Office- und Produktionsnetze zu entkoppeln und sensitive Fertigungslinien vor ungewollten, externen Zugriffen zu schützen. Wir vermitteln die technischen Kompetenzen, um die Sicherheitsstrategien effektiv umzusetzen. Sobald das Verständnis für die Problematik und die notwendige Kompetenz vorhanden sind, steigt auch die Akzeptanz von Sicherheitsmechanismen.“ Zunächst nur für den internen Bedarf vorgesehen, plant Kabatnik, die Schulungen zum Thema IT-Sicherheit in Produktionsumgebungen zukünftig auch für externe Kunden anzubieten.

Kompetente Beratung in allen Projektphasen

Lucia Tandjung ist mit dem Projektergebnis sehr zufrieden: „Die neue Managementplattform für Remote Networks hat unsere Erwartungen voll erfüllt. Wir haben eine verlässliche Grundlage für den weiteren Ausbau der Produktionsnetzwerke geschaffen. Die Hard- und Software ist sehr gut durchdacht, die Komponenten sind optimal aufeinander abgestimmt. Bei anderen Alternativen hätten wir die Applikationen selbst entwickeln müssen. Die Bediensoftware ist benutzerfreundlich konzipiert, sodass auch wenig erfahrene Anwender sie mühelos parametrieren können.“ Tandjung hebt hervor, dass die SCALANCE-Geräte hutschienentauglich sind, DC 24 V-Anschlüsse haben und sehr kompakt gebaut sind, was beim Einbau sehr vorteilhaft ist. „Der Key-Plug ermöglicht eine einfache und effiziente Vorkonfektionierung der SCALANCE-Router. Unsere Kollegen vom Prüfmittelbau liefern so ihre Prüfanlagen betriebsbereit an andere Niederlassungen aus.“

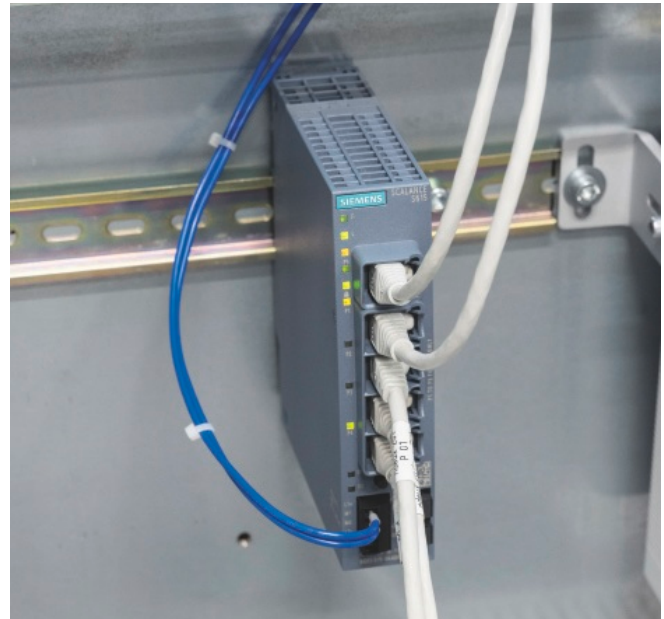


Screenshot der benutzerfreundlichen Oberfläche von SINEMA RC Client

Die Einführung der Managementplattform ließ sich laut Aussage der Festo-Projektleiterin planmäßig umsetzen, was die Leistungsfähigkeit der Siemens-Lösung beweist. Lucia Tandjung fasst zusammen: „Wir haben die vier Anlagen mit dem SCALANCE S615 ins Produktionsnetzwerk eingebunden, ansonsten waren keine zusätzlichen Schritte erforderlich. Wir erhielten in allen Projektphasen sehr kompetente Beratung durch die Siemens-Mitarbeiter.“

Die Managementplattform war zunächst nur für das Werk Scharnhausen geplant. Nun prüft die IT-Leitung, ob sich das Konzept auch für andere Standorte übernehmen lässt. „Was die neue Lösung für die Werksinstandhaltung interessant macht, ist der geringe Zeitaufwand für die Anbindung einer neuen Anlage, der sich „von zwei Wochen auf einen halben Tag verkürzt hat“, berichtet Hieber stolz. „Mit dem SINEMA RC Client lassen sich die einzelnen Ports einfach individuell konfigurieren. „So konnten wir in der Technologiefabrik Scharnhausen mit SINEMA Remote Connect sämtliche Use Cases umsetzen.“

Ohne die neue Managementplattform – darin sind sich die Projektbeteiligten einig – ließe sich das Festo-Portfolio aus IP-fähigen Komponenten und Maschinen nicht effizient administrieren. Es besteht auch nicht mehr die Gefahr, bei Eingabe einer falschen IP-Adresse einen Netzausfall zu verursachen. Der Profinet-Zugriff bietet zudem die Grundlage für weitere Innovationsprojekte wie Energiedaten-Management oder der Einrichtung eines „predictive Maintenance“-Cockpits zum Monitoring von Sensorwerten in einer intelligenten Fabrik.



Die Stationen der Produktionslinie sind mit den Ports des SCALANCE S615 verbunden.

Zusammenfassung

Gesicherter Internet-/Intranetzzugang mit und ohne virtuellen Jump Host:

- Direkter oder nur indirekter Zugang der Instandhalter über Field PG/Notebook (IEC62443)
- Akzeptieren der IT-Remote Access AGBs mit SINEMA Remote Connect
- Zentrale Vergabe der User-Rechte mit SINEMA Remote Connect
- Keine IP-Adresskonflikte oder doppelte Adressen mit NAT (Vorteil bei Serienmaschinen)
- Kein Gewährleistungsverlust, da keine IP-Adressen verändert werden
- Einfache Zellensegmentierung mit NAT, Firewall, VLANs und IPsec
- Zeitersparnis durch Remote-Zugriff der OEMs, bevor die Anlage angeliefert wird
- Gateway mit „DHCP Service Dose“, um IP-Adresskonflikte zu vermeiden

Securityhinweise

Um Anlagen, Systeme, Maschinen und Netzwerke gegen Cyber-Bedrohungen zu sichern, ist es erforderlich, ein ganzheitliches Industrial Security-Konzept zu implementieren (und kontinuierlich aufrechtzuerhalten), das dem aktuellen Stand der Technik entspricht. Die Produkte und Lösungen von Siemens formen nur einen Bestandteil eines solchen Konzepts. Weitergehende Informationen über Industrial Security finden Sie unter <http://www.siemens.com/industrialsecurity>

Siemens AG
Process Industries and Drives
Process Automation
Postfach 48 48
90026 Nürnberg
Deutschland

© Siemens AG 2017
Änderungen vorbehalten
PDF
Referenz
FAV-268-2017-PD-PA
BR 1217 / 6 De
Produced in Germany

Die Informationen in dieser Broschüre enthalten lediglich allgemeine Beschreibungen bzw. Leistungsmerkmale, welche im konkreten Anwendungsfall nicht immer in der beschriebenen Form zutreffen bzw. welche sich durch Weiterentwicklung der Produkte ändern können. Die gewünschten Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart werden. Liefermöglichkeiten und technische Änderungen vorbehalten.

Alle Erzeugnisbezeichnungen können Marken oder Erzeugnisnamen der Siemens AG oder anderer, zuliefernder Unternehmen sein, deren Benutzung durch Dritte für deren Zwecke die Rechte der Inhaber verletzen kann.

Festo Didactic

Der ständig zunehmende Vernetzungsgrad der Fertigung und die damit einhergehenden steigenden Anforderungen an den Schutz der Infrastruktur vor Ausspähung und Manipulation erzeugen auch einen Bedarf an zusätzlichen Kompetenzen bei den Verantwortlichen in der Fertigung. Festo setzt hierbei auf die Dienstleistungen des Schwesterunternehmens Festo Didactic, dem weltweit führenden Ausbilder im Bereich der technischen Bildung. Festo Didactic entwirft und implementiert Bildungslösungen, die Menschen systematisch auf das Arbeiten in dynamischen und komplexen Umgebungen vorbereiten. Ziel ist dabei die Maximierung von Lernerfolgen in Schulen und Lernzentren und die nachhaltige Kompetenzentwicklung in Industrieunternehmen.

Parallel zur Einführung der vorgestellten Fernwartungslösung in der Fertigung von Festo wird auf der Basis der eingesetzten Produkte SINEMA Remote Connect und SCALANCE S615 sowie weiterer Komponenten wie managed Switches der SCALANCE X-Familie ein Schulungsprogramm für Mitarbeiter von Festo angeboten. Den Mitarbeitern aus der Instandhaltung und angrenzenden Berufsfeldern werden dabei Netzwerk- und IT-Security-Inhalte vermittelt, die zum Verständnis und zum Betrieb der eingesetzten Lösung benötigt werden.

Dr. Matthias Kabatnik, verantwortlich für Lernlösungen zum Themenbereich IT-Security bei Festo Didactic, entwickelt das Trainingsprogramm: „Bei der Gestaltung dieses Trainingsangebots haben wir großen Wert auf eine enge Verzahnung von theoretischen und praktischen Bestandteilen gelegt. Um eine möglichst hohe Akzeptanz der Inhalte und einen guten Lernerfolg zu erzielen, werden die Trainingsbeispiele eng mit dem Projektteam abgestimmt. Auf diese Weise entsprechen viele Szenarien konkreten Umsetzungsanforderungen aus dem Projekt und wir erreichen eine sehr hohe Praxisnähe.“

Das Trainingsprogramm beinhaltet Ethernet-Kommunikation, geroutete Netzwerke, VLAN-Konzepte und Sicherheitsmechanismen zur Authentifizierung und zum Aufbau von VPN-Verbindungen, wie sie im Rahmen der Fernwartungslösung eingesetzt werden. Kabatnik betont, dass neben der Vermittlung technischer Grundlagen auch ein Verständnis für die organisatorischen Bestandteile einer Fernwartungslösung als Lernziel wichtig ist, da der sichere Betrieb einer Anlage immer als gesamtheitlicher Prozess betrachtet werden muss. Nur dieses Verständnis führt letztlich zur Akzeptanz von Schutzmechanismen und damit zu deren korrekter Umsetzung. Das zunächst für die interne Qualifizierung bei Festo entwickelte Trainingsprogramm soll voraussichtlich im Jahr 2018 auch Kunden angeboten werden.