




# Neues Fernwartungs- „Rezept“ für die Pharma- produktion

Netzwerk-Managementplattform und Security Modules für komfortablen Fernzugriff (auch) in der Pharmaproduktion

Für einen Dienstleister in Düren gehört zu einem Automatisierungs-Retrofit ein gesicherter Fernzugriff, um hohe Anlagenverfügbarkeit gewährleisten zu können. Er setzt dazu auf Security Modules und eine neue, komfortable Netzwerk-Managementplattform. Damit lassen sich gesicherte VPN-Verbindungen zu diversen Ethernet-Systemen einfach einrichten, verwalten und aufbauen ohne das Betreiber Netzwerk zu beeinträchtigen. Das hat das Retrofit zweier Tablettenpressen bei einem renommierten Pharma-produzenten gezeigt.

Automation, Consulting, Service und Retrofit – Dienstleistungen für Maschinen und Anlagen – vorzugsweise in der Pharmaproduktion – sind das Metier der ACSR-Solutions GmbH aus Düren (Nordrhein-Westfalen). Die Mitarbeiter dort haben zum Teil jahrzehntelange Erfahrung sowohl in der Entwicklung als auch im Bau und im Support der dort eingesetzten Systeme.

Die Dürener haben dafür ein maßgeschneidertes Produktprogramm entwickelt. Es umfasst standardisierte Hard- und Software-Lösungen für den effizienten Betrieb von Tablettenpressen (TabControl), Wirbelschichtgranulierern (FluidBed-Control), Blisterlinien und Kartonierern (PacControl) sowie Mischern (MixControl) praktisch aller Hersteller. Diese bilden den elektronischen Kern bei Retrofit-Projekten und lassen sich mit wenig Aufwand für individuelle Aufgaben konfigurieren. Damit wurden auch schon verschiedene Anwendungen in der Nahrungsmittel- und der chemischen Industrie realisiert.

Die Standards werden regelmäßig überprüft und innoviert, wenn neue Funktionalitäten einen Mehrwert bringen. Wie letztes Jahr, als Siemens mit SINEMA Remote Connect seine neue Netzwerk-Managementplattform für die Fernwartung vorgestellt hat.

### In der Pharmaproduktion im Einsatz

Als einer der ersten Anwender profitiert davon die Aesica Pharmaceuticals GmbH aus Zwickau. Das Unternehmen gehört zur britischen Consort-Medical-Gruppe und produziert für verschiedene Pharmaunternehmen diverse Arzneiwirkstoffe und Bulk-Präparate wie Kapseln, Dragees und Tabletten. Die Produktionskapazität am Standort Zwickau beträgt über drei Milliarden „Einheiten“. Die Produktionsprozesse werden regelmäßig sowohl von Gesundheitsbehörden verschiedener Länder als auch von den Auftraggebern auditiert. Das Qualitätsmanagement entspricht sowohl den deutschen und europäischen Good-Manufacturing-Practice-(GMP)-Standards als auch den Richtlinien zahlreicher Gesundheitsbehörden auf der ganzen Welt – wie der US-amerikanischen FDA.

Entsprechend hoch sind die Anforderungen an die eingesetzten Produktionsmittel und der Aufwand, diese auf hohem technischem Niveau zu halten. Die Sachsen setzen dabei auch auf die Erfahrung und das Know-how der ACSR-Solutions und haben diese mit dem Retrofit zweier Tablettenpressen beauftragt. Eine Einfach- und eine Doppel-Rundläuferpresse sollten mechanisch gründlich überholt, die Elektro- und Automatisierungstechnik wieder auf den neusten Stand gebracht werden. Um die Ersatzteilverfügbarkeit wieder langfristig zu sichern, hat ACSR die ursprüngliche Steuerung beider Pressen durch sein PC-basiertes TabControl-System ersetzt. Die Schaltschränke wurden komplett neu aufgebaut, die Haupt- und Füllschuhantriebe mit kompakten Siemens-Umrichtern SINAMICS G120C ausgerüstet. Als Herzstück für gesicherte Fernwartung wurde in beiden Schränken ein Security Module SCALANCE S615 von Siemens montiert. Die Geräte sind das Bindeglied zur neuen, bei ACSR eingerichteten Netzwerk-Managementplattform SINEMA Remote Connect.



Schnittstelle zum SINEMA Remote Connect bei ACSR sind die Security Modules SCALANCE S615, die sich rückwirkungsfrei ins Betreiber Netzwerk integrieren ließen.

### Komfortabel zur gesicherten Verbindung

Mit SINEMA Remote Connect lassen sich sehr einfach und komfortabel gesicherte Fernzugriffsverbindungen über Virtual Private Network Tunnels (VPN-Tunnel) konfigurieren, verwalten und aufbauen.

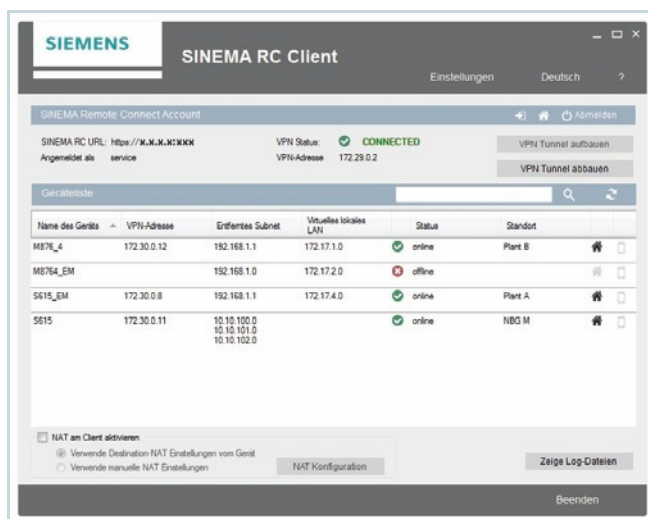
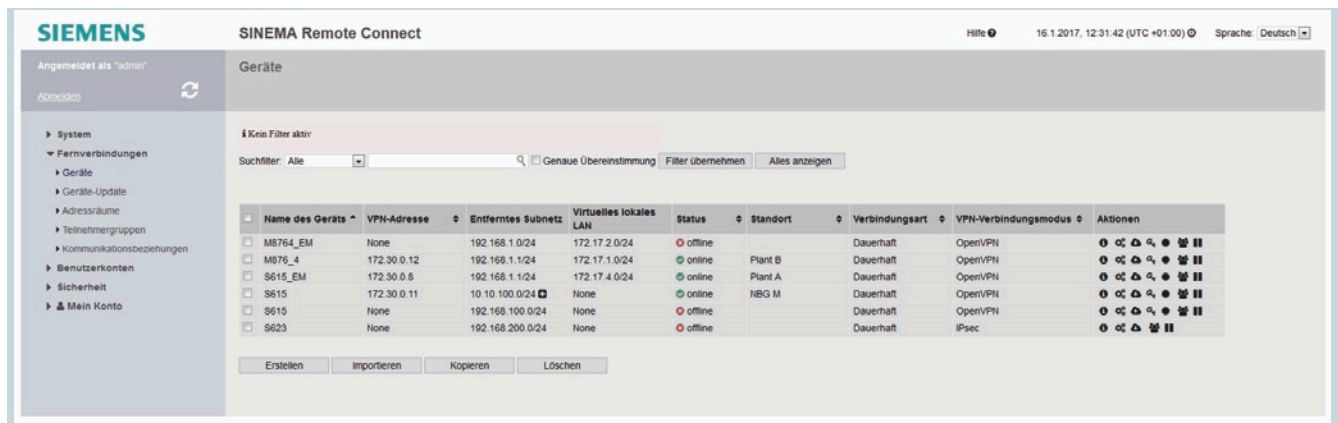
Die Kommunikation zwischen den Netzwerkteilnehmern ist IP-basiert sowie protokollunabhängig und somit universal einsetzbar. Über SINEMA Remote Connect ist der Fernzugriff auf sämtliche kommunikationsfähige Teilnehmer im lokalen Netz möglich. Ein direkter Zugriff auf das Firmennetzwerk, in das eine Maschine oder Anlage eingebunden ist, wird durch die Firewall-Einstellungen des SCALANCE S615 unterbunden und die Netzwerkeinstellungen vorhandener Teilnehmer müssen nicht angepasst werden. „Das war auch für unsere IT-Spezialisten die Voraussetzung dafür, ein solches Fernwartungssystem grundsätzlich zuzulassen“, sagt Andreas Ritter, Technischer Leiter bei Aesica. „Uns gibt das die Möglichkeit, auch für bestehende Anlagen nachträglich eine Fernwartung einrichten zu können, ohne die Produktion unterbrechen zu müssen“, sagt Klaus Rosenbach, für die Automatisierung verantwortlicher Geschäftsführer der ACSR-Solutions GmbH.

Der Servicetechniker und die zu wartende Maschine stellen via OpenVPN getrennt voneinander eine Verbindung zum SINEMA Remote Connect her. Dieser ermittelt über den Austausch von Zertifikaten die Identität der Teilnehmer und gibt nach erfolgreichem Abgleich den Fernzugriff frei. Der Pharmaproduzent geht noch zwei Schritte weiter. Er richtet für Fernwartungsaufgaben eigene VLANs ein und stellt die physikalische Netzwerkverbindung am SCALANCE-Security Module ausschließlich bei Bedarf und nach Rücksprache mit dem Dienstleister her.



Die Schaltschränke bei Aesica Pharmaceuticals wurden komplett neu aufgebaut.





Mit der Server-Applikation lassen sich gesicherte VPN-Verbindungen komfortabel anlegen, konfigurieren und verwalten, im Adressbuch des SINEMA RC Clients einfach auswählen und aufbauen.

Mit der Installation des SINEMA RC Clients steht dem Benutzer eine Adressbuchfunktion zur Verfügung. Darüber kann ein Servicetechniker auch unterwegs für ihn relevante Maschinen und Anlagen eindeutig identifizieren, auswählen und dann fernwarten. Im Serienmaschinenbau – mit gleichen Maschinen und IP-Adressen im Feld – ist das ein entscheidender Vorteil.

Einmal angelegte OpenVPN-Konfigurationen und -Zertifikate lassen sich sehr einfach exportieren und importieren, wenn beispielsweise neue mobile Endgeräte für die Fernwartung genutzt werden sollen.

### Mehrere gesicherte VPN-Verbindungen möglich

Die Verbindung zur Managementplattform für Remote Networks SINEMA Remote Connect kann grundsätzlich über verschiedene Medien, wie Mobilfunk, DSL oder vorhandene Netzwerk Infrastrukturen aufgebaut werden. Siemens bietet für alle Varianten SCALANCE-Router an, die sich per Auto-konfiguration einfach parametrieren und in vorhandene Strukturen einbinden lassen.

So auch die hier prädestinierten Security Router SCALANCE S615. Die Geräte sind DHCP-fähig und können ihre IP-Adresse automatisch vom überlagerten Unternehmens-Netzwerk, das mit dem Internet verbunden ist, beziehen. Auf der Automatisierungsseite des SCALANCE S615 kann jedes Gerät identische IP-Subnetze besitzen, die dann durch Adressübersetzung (1:1 NAT – network address translation) seitens SINEMA Remote Connect eindeutig zugeordnet werden. Die SINEMA Remote Connect Server-Applikation kann eine hohe Anzahl VPN-Tunnel via OpenVPN und IPsec entgegennehmen und verwalten.

„Mit herkömmlichen 1:1 VPN-Verbindungen ist das nicht derart einfach und zugleich gesichert möglich“, so Klaus Rosenbach. „So ließe sich bei Bedarf auch für ein autorisiertes Partnerunternehmen schnell ein abgesicherter Fernzugriff über unseren SINEMA Remote Connect einrichten – von jedem beliebigen Ort mit Internetzugang aus“, so Klaus Rosenbach.

### Abgesicherter Fernzugriff – einfacher, komfortabler und flexibler denn je

Fazit von Klaus Rosenbach: „Die neue Netzwerk-Managementplattform von Siemens macht unsere Arbeit als Dienstleister im Service ein weiteres Stück einfacher und komfortabler. Mit dieser zentralen Server-Applikation und theoretisch beliebig vielen SINEMA RC Clients und SCALANCE S können wir die Anwender unserer Systeme von jedem Ort aus an jedem Ort noch besser und flexibler unterstützen als bisher. Wir können bei Störungen im Betrieb aus der Ferne eingreifen und Stillstandszeiten minimieren, damit die Anlagenverfügbarkeit und die Produktivität hoch halten.“ All das mit der in der Pharmaindustrie gebotenen IT-Sicherheit. Die Zugriffsmöglichkeiten sind flexibel und in jedem Fall abgesichert. Sie haben keinerlei Auswirkungen auf das Betreiber Netzwerk, so dass auch im sensiblen Umfeld der Pharmaindustrie eine hohe Akzeptanz gegeben ist. „Wir werden künftige Modernisierungen sehr wahrscheinlich nach dem mittlerweile bewährten, sicheren Konzept umsetzen“, so Andreas Ritter von Aesica Pharmaceuticals.

## SCALANCE-Netzkomponenten – Sicher und flexibel vernetzt über alle Ebenen

Neben SCALANCE S gibt es mit SCALANCE M auch Mobilfunkrouter im Siemens-Portfolio. Die SCALANCE-Geräte sorgen ganz allgemein für einen gesicherten Zugriff auf weltweit verteilte Anlagen, Maschinen und Applikationen. Sie schützen Automatisierungszellen und alle Komponenten vor unbefugten Zugriffen wie Spionage oder Manipulation. Firewall-Regeln ermöglichen sowohl eine geräte- als auch anwenderspezifische Kontrolle von Zugriffen.

## ACSR-Solutions – individuelle Dienstleistungen (nicht nur) für pharmazeutische Maschinen und Anlagen

Die ACSR-Solutions GmbH ist aus ihrer Historie heraus ein ausgewiesener Spezialist für die Automation, das Consulting, den Service und Retrofits für pharmazeutische Maschinen und Anlagen aller Hersteller. Auch führende Unternehmen der Nahrungsmittel- und der chemischen Industrie setzen die Produkte und Lösungen der Dürer ein.

Ein Schwerpunkt sind maßgeschneiderte, das heißt individuell auf die Wünsche des Kunden abgestimmte Retrofit-Projekte. Diese reichen von der Überholung einzelner Baugruppen über die Erneuerung der Steuerungstechnik bis hin zur Generalüberholung von Maschinen und Anlagen. Dabei setzt ACSR bevorzugt die Produkte der eigenen Automation-Sparte ein.

Ein Retrofit beginnt immer mit einer Analyse der Maschine oder Anlage. Danach erarbeiten die Spezialisten gemeinsam mit dem Kunden die notwendigen Maßnahmen, beschaffen die Komponenten und montieren diese weitestgehend vor. Der Umbau kann wahlweise in Dürer oder vor Ort beim Kunden realisiert werden. Nach dem Factory Acceptance Test (FAT) beim Maschinenbauer folgen die Inbetriebnahme inklusive Kalibrierung, der Site Acceptance Test (SAT) beim Kunden sowie die Qualifizierung und Schulung der Mitarbeiter. Auf alle Maßnahmen gibt der Dienstleister eine Garantie

### 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-30-2017-PD-PA  
BR 0917 / 4 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.