SIEMENS

Reference

# New Remote Maintenance "Recipe" for the Pharmaceutical Production

## Network Management Platform and Security Modules for convenient Remote Access  in the Pharmaceutical Production

For a service provider in Düren, Germany, an automation retrofit includes secured remote access to ensure high equipment availability. To that end, the firm relies on Security Modules and a new, convenient Network Management Platform, which allow secured VPN connections to various Ethernet systems to be easily set up, managed and established without affecting the operator network. This was demonstrated by the retrofit of two tablet presses at a renowned pharmaceutical producer.

Automation, consulting, servicing and retrofit services for machinery and equipment – primarily in the pharmaceutical production – are the domain of the ACSR-Solutions GmbH in Düren (North Rhine-Westphalia, Germany). Some of its employees have decades of experience in the development as well as construction and support of the systems employed.

For that, the company has created a tailor-made product range. It includes standardized hardware and software solutions for the efficient operation of tablet presses (TabControl), fluid bed dryers (FluidBedControl), blister packaging lines and cartoner machines (PacControl), as well as granulators (MixControl) from practically any manufacturer. These form the electronic core for retrofit projects and can be configured with minimal effort for individual tasks. Various applications in the food and chemical industries have also already been implemented.

The standards are regularly reviewed and updated when new functionalities provide added value. Like last year, when Siemens introduced its new Network Management Platform for remote maintenance – SINEMA Remote Connect.

**www.siemens.com/sinema-remote-connect**

### Used in the Pharmaceutical Production

One of the first users to benefit from that is the Aesica Pharmaceuticals GmbH from Zwickau, Germany. The organization belongs to the British Consort Medical Group and produces various active pharmaceutical ingredients and bulk preparations such as capsules, pills and tablets for various pharmaceutical companies. The production capacity at the Zwickau site is over three billion "units". The production processes are regularly audited by health authorities from different countries as well as by the customers. The quality management meets the German and European Good Manufacturing Practice (GMP) standards, as well as the guidelines of numerous health authorities around the world – such as the FDA.

Correspondingly high are the demands on the production equipment used and the effort to keep it at a high technical level. Due to its experience and know-how, ACSR was commissioned by Aesica to retrofit two tablet presses. A single and a double rotary press were to be thoroughly overhauled mechanically, and the electrical and automation technology be brought up to date. To once more ensure the long-term availability of spare parts, ACSR replaced the original control of both presses with its PC-based TabControl system. The control cabinets were completely rebuilt, and the main and feeder drives equipped with compact Siemens SINAMICS G120C inverters. As the centerpiece for secured remote maintenance, a Siemens SCALANCE S615 Security Module each was installed in both cabinets. The devices are the link to the new SINEMA Remote Connect network management platform set up at ACSR.

The control cabinets at Aesica were completely rebuilt.

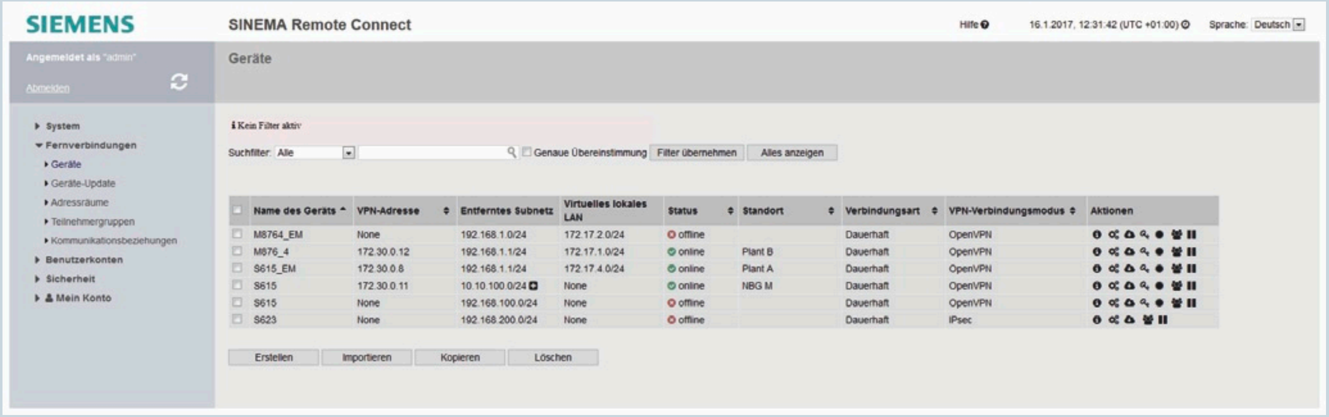
The interface to Simema Remote Connect at ACSR are the SCALANCE S615 Security Modules, which could be integrated reactionless into the operator network.

### Conveniently establishing a secured Connection

With SINEMA Remote Connect, secured remote access connections can be very easily and conveniently configured, managed and established using virtual private network (VPN) tunnels.

The communication between the network participants is IP-based and protocol-independent – and therefore universally usable. Via SINEMA Remote Connect, the remote access to all communication-capable participants in the local network is possible. Direct access to the company network into which machinery or equipment is integrated is prevented through the firewall settings of the SCALANCE S615 – the network settings of existing participants do not have to be adapted. "This was also the prerequisite for our IT specialists to, in principle, permit such a remote maintenance system," says Andreas Ritter, technical director at Aesica. "This gives us the ability to set up remote maintenance for existing plants as well, without having to interrupt the production," says Klaus Rosenbach, managing director of ACSR responsible for automation.

The service technician and the machine to be serviced separately establish a connection to SINEMA Remote Connect using OpenVPN. SINEMA Remote Connect determines the identity of the participants via the exchange of certificates and enables remote access after successful comparison. The pharmaceutical company then goes two steps further. It sets up its own VLANs for remote maintenance tasks and only establishes the physical network connection on the SCALANCE Security Module when necessary and after talking to the service provider.



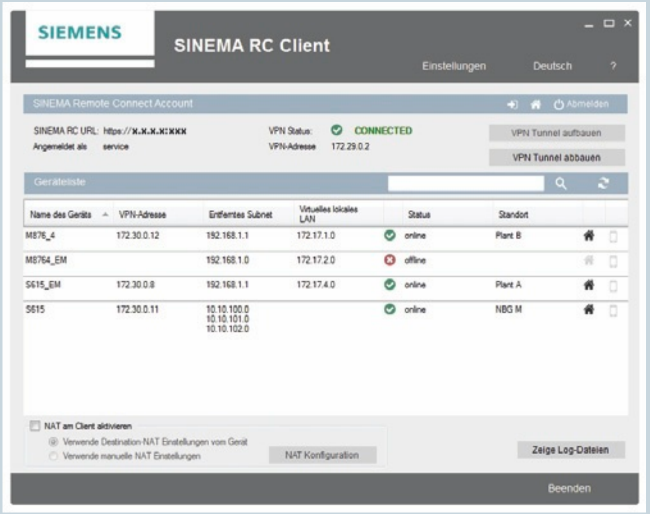
16.1.2017, 12:31:42 (UTC +01:00)

Angemeldet als "admin"

Kein Filter aktiv

Suchfilter: Alle □ Genaue Übereinstimmung

| □ | Name des Geräts | VPN-Adresse | Entferntes Subnetz | Virtuelles lokales LAN | Status | Standort | Verbindungsart | VPN-Verbindungsmodus | Aktionen |
|---|---|---|---|---|---|---|---|---|---|
| □ | M8764_EM | None | 192.168.1.0/24 | 172.17.2.0/24 | offline | | Dauerhaft | OpenVPN | |
| □ | M876_4 | 172.30.0.12 | 192.168.1.1/24 | 172.17.1.0/24 | online | Plant B | Dauerhaft | OpenVPN | |
| □ | S615_EM | 172.30.0.8 | 192.168.1.1/24 | 172.17.4.0/24 | online | Plant A | Dauerhaft | OpenVPN | |
| □ | S615 | 172.30.0.11 | 10.10.100.0/24 | None | online | NBG M | Dauerhaft | OpenVPN | |
| □ | S615 | None | 192.168.100.0/24 | None | offline | | Dauerhaft | OpenVPN | |
| □ | S623 | None | 192.168.200.0/24 | None | offline | | Dauerhaft | IPsec | |



SINEMA RC URL: https://x.x.x.x:xxx
Angemeldet als service
VPN Status: CONNECTED
VPN-Adresse 172.29.0.2

| Name des Geräts | VPN-Adresse | Entferntes Subnet | Virtuelles lokales LAN | Status | Standort |
|---|---|---|---|---|---|
| M876_4 | 172.30.0.12 | 192.168.1.1 | 172.17.1.0 | online | Plant B |
| M8764_EM | | 192.168.1.0 | 172.17.2.0 | offline | |
| S615_EM | 172.30.0.8 | 192.168.1.1 | 172.17.4.0 | online | Plant A |
| S615 | 172.30.0.11 | 10.10.100.0<br>10.10.101.0<br>10.10.102.0 | | online | NBG M |

□ NAT am Client aktivieren
◉ Verwende Destination-NAT Einstellungen vom Gerät
○ Verwende manuelle NAT Einstellungen

With the server application, secure VPN connections can be conveniently created, configured and managed; and be easily selected and established from the address book of the SINEMA RC Client

With the installation of the SINEMA RC Client, an address book function is available to the user. With it, a service technician on the road can clearly identify, select and then remotely service machinery and equipment of relevance. This is a decisive advantage in the construction of identical series machines that have the same IP address in the field.

Once created, OpenVPN configurations and certificates are very easy to export and import, for example, when new mobile terminals are to be used for the remote maintenance.

### Multiple secured VPN Connections possible

The connection to the SINEMA Remote Connect management platform for remote networks can be established using various means such as mobile communications, DSL or existing network infrastructures. For all variants, Siemens offers SCALANCE routers, which can be easily parameterized by auto-configuration and integrated into existing structures.

Just like the SCALANCE S615 Security Modules utilized here. The devices are DHCP-enabled and can automatically obtain their IP address from the higher-level company network, which is connected to the Internet. On the automation side of the SCALANCE S615, each device can have identical IP subnets, which are then clearly assigned through address translation (1:1 NAT – network address translation) by SINEMA Remote Connect. The SINEMA Remote Connect server application can receive and manage a large number of VPN tunnels via OpenVPN and IPsec.

“With conventional 1:1 VPN connections, this is not so easy and secure,” states Klaus Rosenbach. “If required, secured remote access for an authorized partner firm could be quickly set up via our SINEMA Remote Connect – from any location with Internet access,” explains Rosenbach.

### Secured Remote Access – with greater Ease, Convenience and Flexibility than ever before

Conclusion of Klaus Rosenbach: “The new Network Management Platform from Siemens makes our work as service provider in the field of servicing easier and more convenient. With this central server application and, theoretically, any number of SINEMA RC Clients and SCALANCE S Security Modules, we are able to even better and more flexibly support our system users located anywhere from anywhere. We can remotely intervene in case of malfunctions and minimize downtimes to keep equipment availability and productivity high.” All this with the IT security necessary in the pharmaceutical industry. The access options are flexible and always secured. They have no impact on the operator network – resulting in a high degree of acceptance in the sensitive environment of the pharmaceutical industry. “We are very likely to implement future modernizations with the now proven, secure concept,” states Andreas Ritter of Aesica Pharmaceuticals.

## SCALANCE Network Components – secured and flexible Networking across all Levels

In addition to SCALANCE S, the Siemens portfolio also contains mobile communications routers with SCALANCE M. Generally speaking, the SCALANCE devices provide secured access to globally distributed machinery, equipment and applications. They protect automation cells and all components against unauthorized access such as espionage or manipulation. Firewall rules permit a device-specific as well as user-specific access control.

## ACSR-Solutions – customized Services (not only) for Pharmaceutical Machinery and Equipment

Based on its history, the ACSR-Solutions GmbH is a proven specialist for the automation, consulting, servicing and retrofitting of pharmaceutical machinery and equipment from any manufacturer. Leading companies in the food and chemical industries also employ the products and solutions from the company based in Düren, Germany.

A focal point are tailor-made, i.e., to the customer's specifications, retrofit projects. These range from the overhaul of individual assemblies to the modernization of the control technology to the general overhaul of machinery and equipment. In doing so, ACSR prefers to use products from its own automation division.

A retrofit always begins with an analysis of the machinery or equipment. Afterwards, the specialists work out the necessary measures together with the customer, procure the components and pre-assemble them as far as possible. The conversion can take place in Düren or on-site at the customer. This is followed by the factory acceptance test (FAT) at the machine builder, the commissioning including calibration, the site acceptance test (SAT) at the customer, and the training and qualification of the employees. ACSR provides a guarantee for all steps.

## Security information

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions only form one element of such a concept. For more information about industrial security, please visit **http://www.siemens.com/industrialsecurity**

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

© Siemens AG 2017
Subject to change without prior notice
PDF
Reference
FAV-30-2017-PD-PA
BR 0917 / 4 En
Produced in Germany

The information provided in this catalog contains merely general descriptions or characteristics of performance which in case of actual use do not always apply as described or which may change as a result of further development of the products. An obligation to provide the respective characteristics shall only exist if expressly agreed in the terms of contract. Availability and technical specifications are subject to change without notice.

All product designations may be trademarks or product names of Siemens AG or supplier companies whose use by third parties for their own purposes could violate the rights of the owners.

**siemens.com/sinema-remote-connect**