SIEMENS

Reference

Maximum Security in the Production Network

Cell Segmentation of Production Facilities as well as secured Internet and Intranet Access thanks to Management Platform for Remote Network

The Festo AG has set up a new security platform for the production automation at its technology factory in Scharnhausen, Germany. Functions such as firewall and VPN encryption provide increased protection during data transmission and seal off the production networks from unauthorized internal and external access. This improves the process reliability and boosts the productivity of the entire production environment.

The Festo AG is a global player in the field of pneumatic and electrical automation technology. The company, based in Esslingen on the Neckar river (Germany), delivers about 33,000 catalog products and ready-to-install automation systems to its customers worldwide. Each year, about 15,000 tailor-made solutions are developed and produced. In addition to automation technology, Festo is focusing on digitalization. This is not just limited to intelligent products, but also covers the entire value chain from the planning phase to components and systems to the production and predictive maintenance. Particularly hardware and software play an important role here – in order to securely network the production systems and thus make possible Industrie 4.0.

"The digitalization of industrial automation systems is associated with increasing networking, large amounts of data and the use of open standards, with which consistency is achieved," describes Albrecht Salm, Chief Information Security Officer at the Festo AG. "The downside of this development is the vulnerability of systems to cyber attacks. The networks in the production area have become targets; the actions by the hackers are becoming increasingly aggressive."

"We have implemented a solution that ensures a secure remote access to machines and production facilities."

Albrecht Salm, Chief Information Security Officer at the Festo AG.

With industrial remote access, the Festo AG has realized its idea of a secured, networked production environment. Salm continues: "Employees in the areas of global IT and maintenance have implemented a solution that not only enables machines and production facilities plus their applications to communicate with each other, but also ensures a secure Internet and intranet access to, for example, the programmable logic controller (PLC) of the machines."

A major challenge for the factory maintenance is the wide variety of network components and routers in the systems, which are not patchable and represent an insecure "black box" for Festo.

"The new management platform for the production networks has fully met our expectations. In addition to the integrated authorization management, key-plug and ports of the routers can be easily and efficiently configured."

Lucia Tandjung, project manager of Festo Global IT.

Reliable Processes throughout the entire Production Network

"In the area of operational technology (OT), we reached a point where it became necessary to make the production networks more secure and centrally administrable," explains Lucia Tandjung, project manager of Festo Global IT.

"Until this point, there was no uniform remote access standard. The stated goal was to considerably restrict the access to the machine tools by external and internal service personnel. Production networks form the backbone of our automation environments. An external technician inadvertently introducing a virus into the network with a service notebook could potentially lead to a 'blaze' paralyzing the plant network of the entire factory," points out the Festo project manager.

"Even before the project start, the office and production networks were separated from one another so that access from the production environment to the office network was not easily possible. With the construction of the new technology factory, the segmentation of the production networks was tackled," describes Matthias Hieber, project manager of Festo Maintenance and responsible for plant connectivity.

"The capability portfolio of the automation components and the engineering framework offers the opportunity to optimally solve our tasks."

Matthias Hieber,
project manager of Festo Maintenance and responsible plant connectivity.

"A security audit of the previously employed remote maintenance solutions revealed that the separation of both networks alone did not meet the high security requirements."

The project team therefore simultaneously planned a further fine segmentation to also completely isolate individual production facilities or individual legacy components. "The increased security requirements demanded a managed central access, which is maintained by the service personnel with internal and external user rights – and not by a multitude of various gateways, whose access rights are partly unknown," says Hieber.

For the manufacture of precision components, Festo employs production islands. The machines are integrated into the production network and protected against unauthorized access via the SCALANCE S615.

Manufacturers have individual remote maintenance solutions for their machine tools and set up plant sections as network components, which makes maintenance work ever more complex. Hieber continues: "Until the introduction of the new security platform, the machines were able to connect to the Internet on their own. Manufacturers equipped their systems with cellular modems, through which they sent alarm messages by SMS or e-mail, for example, based on limit values. But also for each adjustment the machine manufacturers directly dialed into the Festo network. Our maintenance personnel could not remotely access internal plant components and in some instances had to first log in at the manufacturer to perform PLC program changes and status queries. From there, the connection went back to the respective machine in the factory."
This procedure was very insecure and prompted the project team to ask manufacturers to rearrange the IP addresses of their machines according to Festo specifications.
This solution, however, was not feasible in most cases. Furthermore, changing IP addresses could invalidate the warranty of the systems.

Elimination of IP Address Conflicts and Segmentation of Profinet devices

"The introduction of the Siemens solution has eliminated the IP address conflicts," emphasizes Lucia Tandjung. "The use of the SINEMA Remote Connect management platform offers us as well as the machine suppliers the advantage that IP addresses no longer need to be modified. All plant accesses now only run via SINEMA Remote Connect with a central IP address for the access from outside." The new server application receives all tunnel connections (VPN) and thus mediates between the client PCs of the external service technicians and the machines. The communication is protocol-independent, non-proprietary and IP-based.
A direct and uncoordinated access to the production networks is avoided.

With the SINEMA RC client, an address book function is also available, through which machinery and equipment in the technology factory can be uniquely identified and be selected for the secured remote access. The machines are installed by the equipment manufacturer with unchanged IP addresses and connected to the network via the SCALANCE S615 security appliance. SCALANCE S615 also handles the translation of the IP addresses (network address translation, NAT) so that two different networks (internal and external) can be connected via a firewall.

The machines in the production area are not directly accessible from the outside, because they are concealed by NAT plus a firewall. Incoming data packets that come from an external network and are directed to an external IP address of the machine (destination IP address) are replaced in SCALANCE S615 by the internal IP address. Only a few Profinet devices are allowed to communicate with the Festo office network or applications via IP. Even the early and sometimes necessary remote access to new systems that are still in the production phase at the OEM can be realized with the security appliances.

First of all, the Festo maintenance personnel equipped a valve production line with SINEMA Remote Connect. The production line includes a CNC rotary transfer machine for the drilling and turning of the workpieces, a machine for the high-pressure deburring, a handling robot and a system for the feeding and removal of the workpieces. The individual stations are connected to the ports of the SCALANCE S security appliance. The security appliance communicates with the management platform via an encrypted VPN tunnel. For servicing, the VPN tunnel can be activated via a key-operated switch at the SCALANCE S, or the remote user is temporarily activated on the SINEMA Remote Connect management platform. Similar to a USB stick, but without the risk of being infiltrated by viruses, a key-plug stores all configuration data of the security appliances, which makes possible a quick and uncomplicated device exchange during production operation.

The SCALANCE S615 security appliance, the SIMATIC S7-1500 controller and the SITOP PSU8200 power supply are components installed in the control cabinet at Festo.

In combining the SIMATIC S7-1500 machine controllers and the HMI panels from the SIMATIC portfolio with the TIA Portal engineering framework, the high efficiency and flexibility of the solution took center stage in the decision making process. Externally, only the screen and keyboard data of a Festo maintenance engineer are transmitted, since the access to the plant cell by external users takes place only via a virtual jump host computer, where also the TIA Portal is available as a floating license for the parameterization of the facilities. The remote session is also recorded on video for audit security, and the projects are centrally backed up on a Festo backup server. An external field PG or notebook is decoupled from the Festo network thanks to this two-stage remote maintenance concept.

Festo project manager Hieber: "The capability portfolio of the automation components and the engineering framework offers the opportunity to optimally solve our tasks. Thanks to the easy handling, we can very quickly obtain the desired results," says the technical project manager and IT specialist.

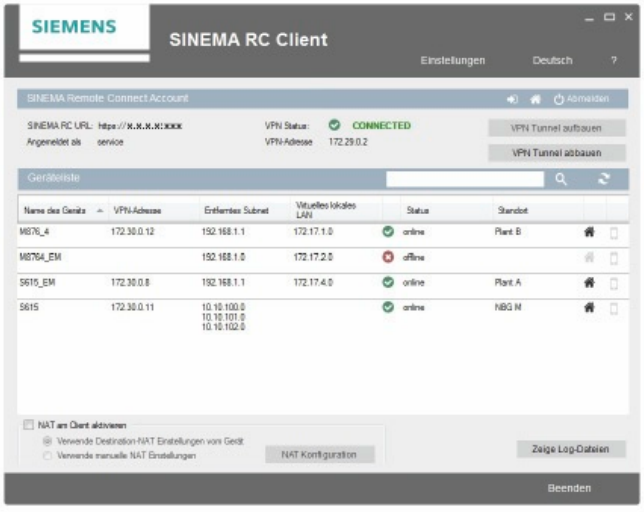
Festo Didactic Training with SINEMA Remote Connect and SCALANCE Switches

In parallel to the introduction of this remote maintenance solution in the production, Festo Didactic SE offers a training program for Festo employees, which is based on the products used including SINEMA Remote Connect and SCALANCE S615 as well as other components such as managed switches of the SCALANCE X family. Employees from maintenance and related occupational fields are taught network and IT security contents, which are needed to understand and operate the solution deployed.
"To familiarize Festo employees with the security-relevant aspects of the production environment, we developed the training program using SINEMA Remote Connect and SCALANCE," explains Dr. Matthias Kabatnik, responsible for IT security learning solutions in the Global Solution Center at Festo Didactic.

"We inform about the necessity to decouple office and production networks, and about the protection of sensitive production lines against unwanted external access. We convey the technical skills needed to effectively implement the security strategies. As soon as there is an understanding of the issue and the necessary competence is available, the acceptance of security mechanisms increases as well."
Initially intended only for internal use, Kabatnik plans to offer the training courses on IT security in production environments also for external customers in the future.

Competent Advice in all Project Phases

Lucia Tandjung is very satisfied with the results of the project: "The new management platform for remote networks has fully met our expectations. We have created a reliable basis for the further expansion of the production networks. The hardware and software are very well thought out, the components are optimally matched to each other. With other alternatives, we would have had to develop the applications ourselves. The operating software is designed to be easy to use so that even less experienced users can effortlessly parameterize it." Tandjung highlights that the SCALANCE devices are DIN rail compatible, feature 24 V DC connections and are built very compact, which is very advantageous during installation. "The key-plug enables an easy and efficient prefabrication of the SCALANCE routers. Our colleagues from the test equipment construction department are thus able to deliver their test systems to other plant locations ready for operation."

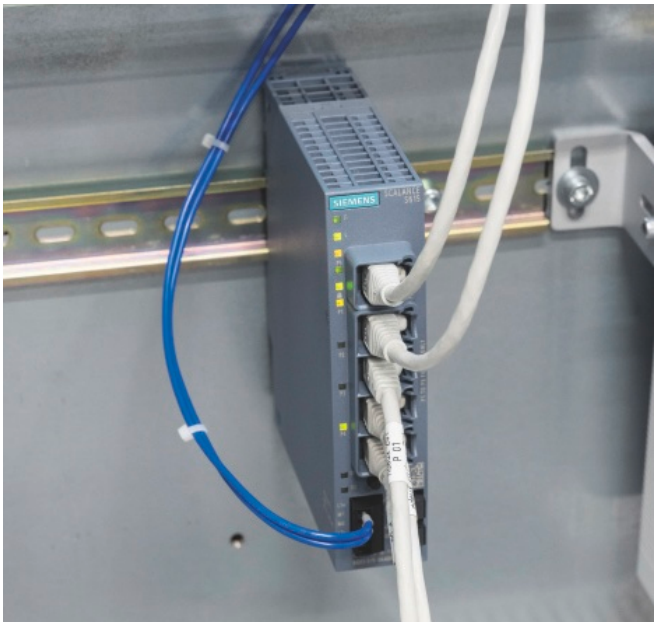


Screenshot of the user-friendly interface of the SINEMA RC Client.

According to the Festo project manager, the implementation of the management platform went as scheduled, which proves the efficiency of the Siemens solution.
Lucia Tandjung summarizes: "We integrated the four facilities with the SCALANCE S615 into the production network, other than that, no additional steps were required. In all project phases, we received very competent advice from Siemens employees."

Initially, the management platform was only planned for the Scharnhausen factory. The IT management is now checking whether the concept can also be adopted by other locations. "What makes the new solution interesting for factory maintenance is the little time required to connect a new plant, which has come down from two weeks to half a day," reports Hieber proudly. "With the SINEMA RC Client, the individual ports can be easily customized. That is how we were able to implement all use cases in the Scharnhausen technology factory with SINEMA Remote Connect."

The project participants agree that without the new management platform, the Festo portfolio of IP-capable components and machines could not be efficiently administered. There also is no longer the risk of causing a network outage when entering an incorrect IP address. Furthermore, the Profinet access provides the basis for further innovation projects such as energy data management or the creation of a predictive maintenance cockpit for monitoring sensor values in an intelligent factory.



The stations of the production line are connected to the ports of the SCALANCE S615.

Summary

Secured Internet/intranet access with and without virtual jump host:

- Direct or indirect access by maintenance personnel via field PG/notebook (IEC62443)
- Acceptance of the IT remote access terms and conditions with SINEMA Remote Connect
- Central allocation of user rights with SINEMA Remote Connect
- No IP address conflicts or duplicate addresses with NAT (advantage with standardized machines)
- No loss of warranty, since no IP addresses are changed
- Easy cell segmentation with NAT, firewall, VLANs and IPsec
- Time saving through remote access by the OEMs before the equipment is delivered
- Gateway with "DHCP Service Dose" to avoid IP address conflicts

Festo Didactic

The ever-increasing degree of networking in manufacturing and the associated increasing demands on the protection of the infrastructure against espionage and manipulation also create a need for additional competencies among those responsible for the production. In this connection, Festo relies on the services of its sister company Festo Didactic, the world's leading provider of technical education. Festo Didactic designs and implements educational solutions that systematically prepare people to work in dynamic and complex environments. The goal is to maximize learning outcomes in schools and learning centers, and to develop lasting competence in industrial companies.

In parallel to the introduction of the presented remote maintenance solution in the production of Festo, a training program for Festo employees is offered based on the products used including SINEMA Remote Connect and SCALANCE S615 as well as other components such as managed switches of the SCALANCE X family. Employees from maintenance and related occupational fields are taught network and IT security contents, which are needed to understand and operate the solution deployed.

Dr. Matthias Kabatnik, responsible for learning solutions on the topic of IT security at Festo Didactic, is developing the training program: "In designing this training program, we placed great emphasis on a tight integration of theoretical and practical components. To obtain the highest possible acceptance of the contents and a good learning outcome, the training examples are closely coordinated with the project team. Many scenarios thus correspond to concrete implementation requirements from the project, and we achieve a very high practical relevance."

The training program is comprised of Ethernet communication, routed networks, VLAN concepts and security mechanisms for authenticating and establishing VPN connections as used in the remote maintenance solution. Kabatnik emphasizes that in addition to conveying technical basics, the understanding of the organizational components of a remote maintenance solution also is an important learning objective, since the safe operation of a plant always has to be regarded as a holistic process. Only this understanding ultimately leads to the acceptance of protective mechanisms and thus to their correct implementation.
The training program initially developed for the internal qualification at Festo is expected to be offered to customers in 2018.

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

PDF
Reference
FAV-268-2017-PD-PA
BR 1217 / 6 En
Produced in Germany

siemens.com/remote-networks