Technical article

Secure and demand-based remote access:
Zero Trust strengthens cell protection

Home office, remote access, Cybersecurity: what in many companies is already part of everyday life on the IT side, creates desire in the OT community. In the industrial production and development environments, too, various jobs can and should be done externally, and certain processes be prepared, initiated, and monitored. Just as dynamic and secure? Siemens and Zscaler Inc. have tackled this task together and combined proven perimeter-based cell protection with flexible Zero Trust principles.

It was only a matter of time anyway, before mobile working, which is widespread in the office/IT world – from the home office or office, remotely in general – would also be demanded by OT (Operational Technology), industrial automation, and network technology. Especially since both worlds are becoming more and more intertwined and IT already has to implement secure access to the OT within the company. The pandemic has further increased the desire of many process and plant operators for more flexible and secure access options from the outside, beyond classic remote maintenance. Siemens, a leading provider of industrial network technology, and Zscaler Inc., a leading provider of a cloud-based security platform, have thus teamed up to solve the relevant tasks.

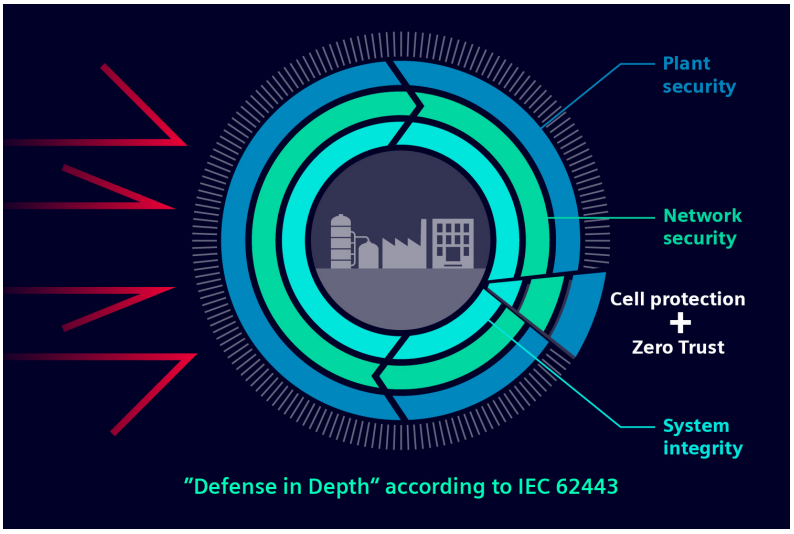
SIEMENS

siemens.com/zero-trust

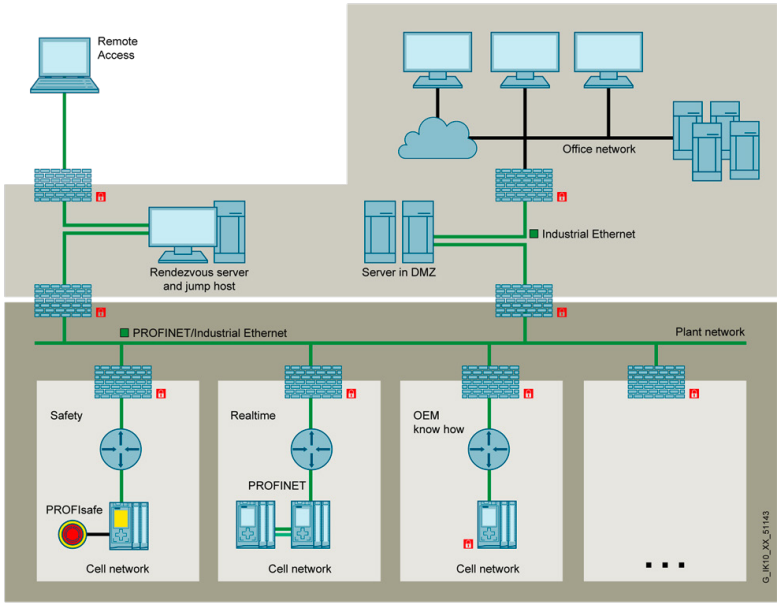
OT is not IT – not all networks are the same

Heterogeneous industrial communication networks, which have often grown over years, have completely different requirements than pure IT solutions in many respects. For instance, data in production must frequently be communicated deterministically in real time. In addition, safety functions must often be implemented at the same time and maximum availability and also know-how protection be ensured. Furthermore, older components sometimes communicate completely open and unencrypted. To fend off cyber attacks, protection concepts tailored to the industry have been developed, such as the "Defense in Depth" concept – the nested defense according to IEC 62443. The network security is based on an individual risk assessment and segmented networks with production cells separately protected by their own firewalls. In such a perimeter-based network, communication from/to the office network or the Internet runs through a so-called demilitarized zone (DMZ) or special rendezvous servers and jump hosts.

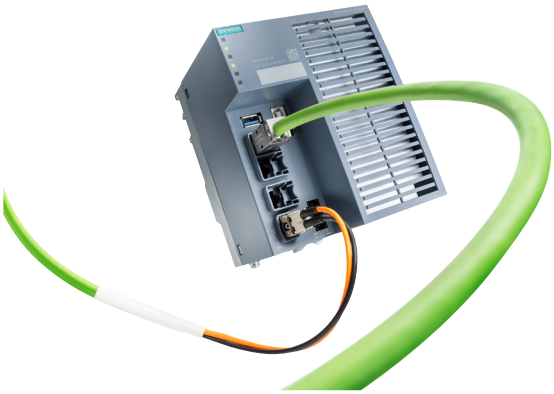
In office networks, with countless, mostly newer devices and constant changes, a protection concept has often been established, in which quite simply no participant is trusted ("never trust, always verify"). This approach, known as "Zero Trust", requires that all network participants – users and devices – always prove their identity and integrity before communication with the desired target resource is established. Many existing automation components and network infrastructures are not equipped to handle this. Therefore, the more flexible, easy-to-use – since it is managed centrally and company-wide – Zero Trust concept cannot be fully transferred or extended to industrial networks without adjustments.



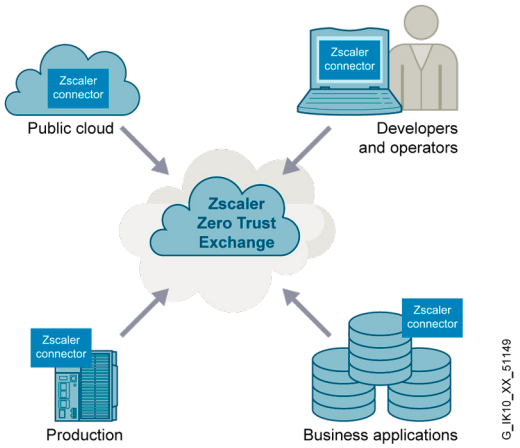
Zero Trust and cell protection as fixed components of the Defense in Depth concept, which adopts both technical and organizational measures to protect production facilities from cyber attacks



Classic perimeter-based approach with remote access via rendezvous server and jump host to segmented OT network with separate "trustworthy" cells secured by their own firewalls



SCALANCE LPE is a small and robust local processing platform with a high-performance CPU. It can be used flexibly, e.g., for edge applications with which plant efficiency can be significantly increased.



Zscaler Zero Trust Exchange enables administrators to centrally define user-specific rule sets in the Zscaler cloud platform, which control the application-specific access to the corresponding target resources.

Intelligently combined to form convergent solutions

To promote the integration of OT and IT nonetheless, Siemens and Zscaler have bundled their competencies for an end-to-end Zero Trust OT/IT security approach. The local processing platform SCALANCE LPE (local processing engine) from Siemens serves as high-performance hardware in the harsh production environment, directly at or also in the production cells. Its actual core task is to collect data and preprocess it close to the process. For this, the device is simply integrated into an existing cell network secured by a firewall via Ethernet.

With its open Linux-based operating system and a powerful CPU, the local processing platform is predestined for the secure, reliable operation of additional applications. In this case, thanks to the app connector of the cloud-based remote access service Zscaler Private Access (ZPA), which can be quickly and easily installed as a Docker container. Using the Zscaler app connector, each SCALANCE LPE can be initially added to and configured in the Zero Trust Exchange cloud platform. It then acts as a Zero Trust gateway for its cell, which is considered intrinsically trustworthy. The Zero Trust Exchange platform monitors all rule sets required for access and provides the interfaces for various identity providers. It only grants uniquely identified and authorized participants access to the resources enabled for them.

In this way, company-wide managed users can access local production or development systems flexibly, demand-based, and securely also from afar, without exposing these systems to an increased threat potential. Thanks to specific authorization concepts, the special requirements of real-time or safety applications as well as of availability and know-how protection can be ensured without having to fundamentally change the architecture of the industrial network. The central management in the Zero Trust Exchange platform and exclusively outgoing connections reduce existing firewall rules and thus also the costs for administration and monitoring. In other words: although additional connections are set up for the interaction of OT and IT, firewall rule sets can be configured more restrictively.

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 constitute one element of such a concept. For additional information on industrial security measures that may be implemented, please visit
www.siemens.com/industrialsecurity

Published by
Siemens AG

Digital Industries
Process Automation
Östliche Rheinbrückenstr. 50
76187 Karlsruhe, Germany

PDF
Technical article
DI PA-2122-2
PDF 1121 4 En
Produced in Germany

Convincing in-house tests – roll-out started

This collaboration was preceded by a large-scale test with several hundred thousand Zscaler participants in the IT network from Siemens. On the same basis, various projects in the areas of development and quality assurance were successfully implemented in own production networks.

Now it is important to define further suitable applications in the production and development environments and to implement specific solutions for them. The focus is initially on companies that already rely on the Zscaler platform for IT and on network technology from Siemens in the production. They can implement the new approach without much effort or fundamental changes to the network infrastructure – and thus benefit from the advantages.

This enables them to realize convergent corporate networks with uniform IT/OT security guidelines for their office and production networks. And ultimately, higher Cybersecurity, flexibility, and efficiency when it comes to mobile working in production and development.

Existing solutions can still be used

The special framework conditions of industrial communication speak for implementing Zscaler and Zero Trust principles as add-on to previous concepts – in order to act more flexibly and dynamically. The "Defense in Depth" concept thus remains in place and will be expanded to include Zero Trust functionalities for network security. Classic VPN-based remote access and the associated management platform will also continue to exist and be further developed in the future. Depending on the industry, application, or company policy, both concepts offer corresponding advantages. In the long term, end-to-end Zero Trust concepts will not only reduce operating costs, but also contribute to greater Cybersecurity in the production environment.