SIEMENS

OPPOSITES ATTRACT

Exploring why IEC 62443 and Zero Trust can be a great match.

Cybersecurity for Industrial Networks

www.siemens.com/zero-trust

WHITEPAPER 2023

Malware outbreaks, industrial espionage and even cyber warfare – the list of threats endangering industries, critical infrastructures and even an entire society's wealth is very long. In reaction, many governments have already passed corresponding cybersecurity resilience acts to protect their economies, environments and people. Consequently, many operators of industrial environments, especially those of critical infrastructures, often turn to the IEC 62443 standard series for guidance around cybersecurity. As recent attacks on oil and gas supplies, power supplies or even satellite systems for whole wind farms have shown, cyber attacks on critical infrastructure or digitalized factories can be devastating. These range from beyond the common economic consequences seen in IT-side cyber attacks to include potential environmental harm, public safety risks and even loss of life.

IEC 62443: an international series of standards for cybersecurity

The IEC 62443 assembles guidance to address not only the industrial technology systems in place but also the people, processes and countermeasures surrounding them. It is a consensus-driven, international community standard that uses a risk-based approach to cybersecurity to help operators protect their valuable assets and prevent the exploitation of vulnerabilities. Its premise rests on a Defense in Depth concept that is deeper than just a single perimeter, relying on multiple layers of security controls to protect valuable OT assets.

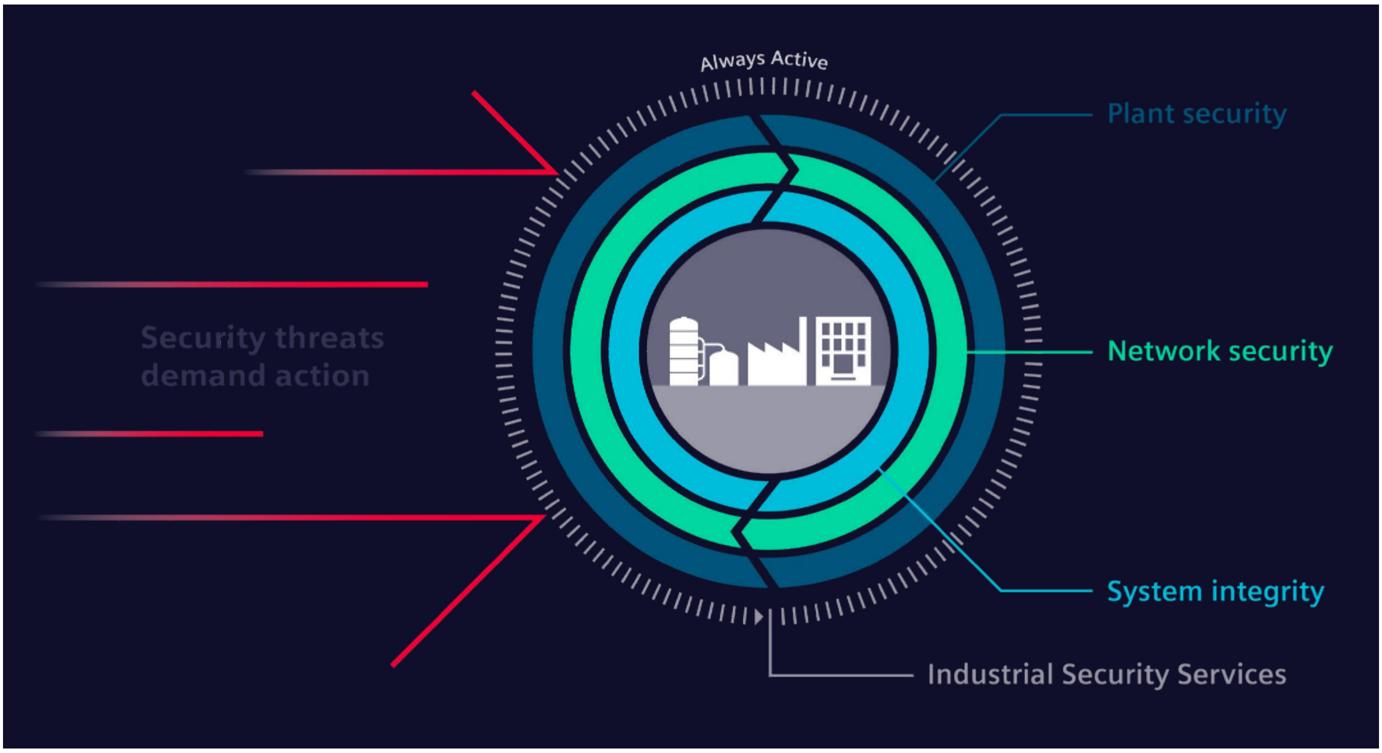
With the trends of Industry 4.0 and factory digitalization, we are now seeing increased IT/OT convergence, which has implications on the guidelines set forth via the IEC 62443. Traditionally, the IEC 62443 promotes complete separation of the OT from IT networks. However, this can create limits to innovation and improvement. For example, integrating IT systems into the OT side helps factories use innovations on the IT side, such as Artificial Intelligence (AI), Machine Learning (ML) and cloud services. These improve agility and output, providing industrial customers with more value and better business profit.

From a security standpoint, there are benefits of bringing IT security principles to the table as well. They can offer much-needed security modernization to prevent against the dreaded ransomware, denial-of-service and other attacks. For example, while VPNs and specific jump host solutions are the current recommended methods to provide secure remote access to factories, the experience has shown that they are only as secure as their latest patch not to mention cost and scalability issues. Additionally, the 'cloudification' highlights the further limitations of classical perimeter-based security concepts as many connections must be monitored and controlled by different levels of firewalls.

Zero Trust: unleashing the potential of "never trust, always verify"

All of the above is exactly why Zero Trust, the latest in the most highly-touted IT architectural principles, holds promise for the OT side. Zero Trust network access, when applied instead of VPN, reduces lateral movement, eliminates the attack surface, creates segmentation and fundamentally relies on multi-factor authentication, a high standard for identity assurance. To explain it in a few words, it operates like an exchange service similar to the telephone exchanges present in the 1940s, where two connections are stitched together on demand.

For instance Zscaler's cloud-delivered Zero Trust solution uses 150+ data centers worldwide to deliver centralized policy and administration control to customers and the micro tunnels they create between users and devices, or applications are fully encrypted. Here it is completely irrelevant where the target resources are located – in IT or even OT space. With Zero Trust network access, an ideal concept was established modernizing security and enabling the IT-OT worlds to collaborate with reduced risk and greater confidence.



The Cybersecurity concept "Defense in Depth" provides comprehensive protection as recommended by the international standard IEC 62443 on three levels: plant security, network security, and system integrity.

Challenges lead to opportunities

Unfortunately, there are some major differences between OT and IT, which are preventing the roll-out of application-specific, Zero Trust network access – down to every single end device. It needs to be considered that OT environments often rely on devices that have been operating for several decades and cannot be easily replaced. These 'legacy' devices were designed in times where nearly no one considered any cyber threats. But even some more modern devices lack security functions like encryption capabilities, integrity protection or providing their unique identities for any authentication purposes, which is an important prerequisite for Zero Trust.

With IEC 62443, a standard was written addressing all specific requirements of an industrial control system. Even if the IEC 62443 does not reflect the principles of Zero Trust – the concept was simply not yet defined when the standard was written – and even if it is based on the traditional Defense in Depth concepts, it is not outdated. The core principles of a layered Defense in Depth architecture are not just moats and walls representing firewalls and network segments – it is much more. With Defense in Depth, many versatile measures are described. Holistic security requires guidelines and policies, in addition to physical perimeter protection, such as simple fences and video surveillance, and even integrity protection mechanisms of used devices. Therefore, Defense in Depth does not mean to add a second or third lock to an entrance door, but rather to add different measures such as motion detectors or video surveillance to prevent a burglar to enter a house. This lock analogy strongly reflects the perimeter-based protection concepts, which are less powerful than a Zero Trust Network Access. It's critical to figure out how to utilize the advantages of Zero Trust in OT while eliminating the gaps of perimeter-based defense. The benefit of an untrusted enterprise network comprising IT and OT with authorized and verified accesses are clearly obvious – higher security postures and only one single management system.

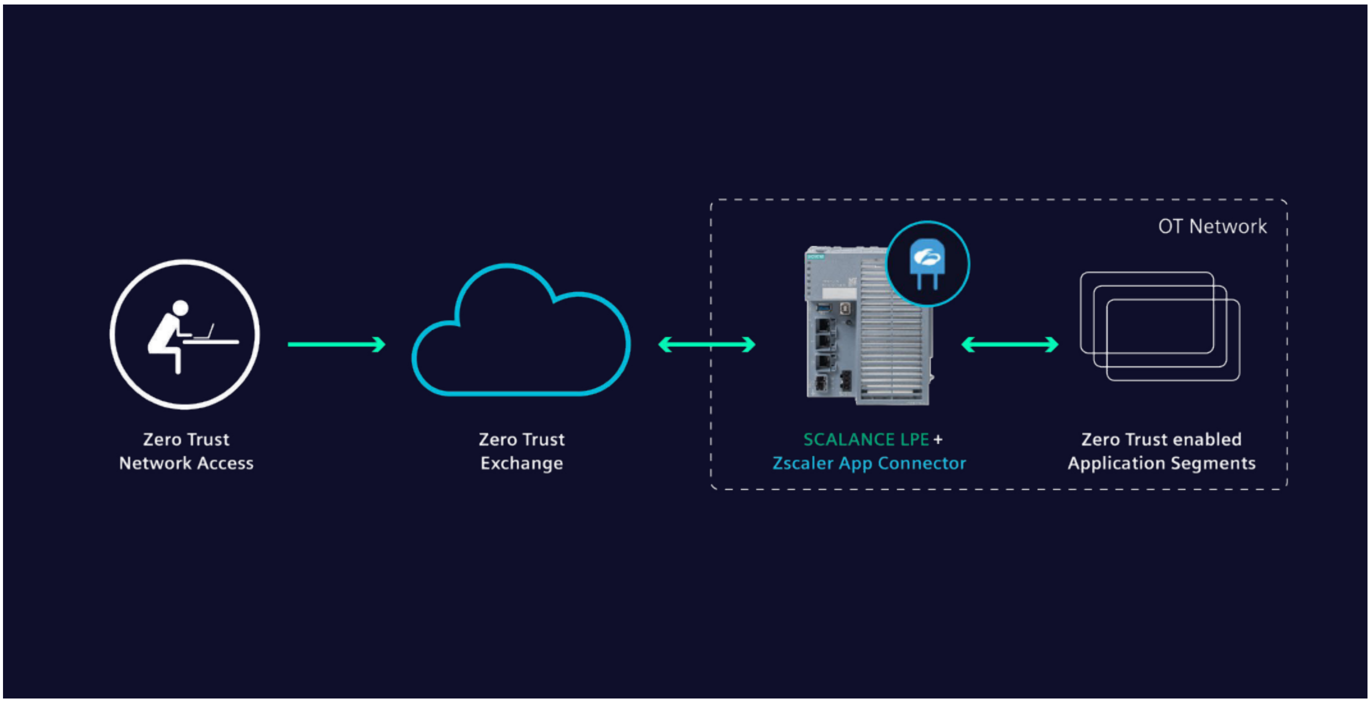
However, some challenges must still be overcome to combine IEC 62443 and Zero Trust network access. There are several restrictions in IEC 62443 and OT architectures, preventing the replacement of network cells and firewalls with Zero Trust. One area that it is at odds with the IEC62443, however, concerns network segmentation and the restriction of data flows. Part 2-1 of the mentioned standard, which requires the establishment of a security program for automation control systems, demands a segmented network architecture as well as a segmentation or even isolation of critical parts of the control systems. To do so, the standard refers to so-called 'barrier devices' that are employed to block non-essential communication. These requirements are additionally reflected in part 3-3 demanding a system security architecture for industrial communication networks.

A network segmentation is also demanded with the fifth foundational requirement addressing the restriction of data flows. Depending on the target security level which shall be achieved, a different set of requirements needs to be fulfilled. This includes, amongst others, physical and logical isolation of critical network segments, protection of zone boundaries as well as separation of production networks and non-control networks, such as the office environment. If these requirements are fulfilled, the OT-specific requirements such as ensuring safety and determinism can also be fulfilled.

In conclusion, the major challenges can be summarized as follows:

– Network segmentation according to security levels
– Protection of zone boundaries and restriction of data flows
– Separation of IT and OT networks
– Isolation of critical network segments

Besides these challenges, there are also some requirements for which a Zero Trust based solution would be predestined. User access and user authentication are requirements also described in IEC 62443-2-1 and 3-3, which challenges every perimeter-based security architecture – especially for remote users. Depending on the target security levels, these requirements comprise an authentication of all users before a system can be used, re-authentication, full logging of access attempts and also authentication for a so-called 'task-to-task communication'. Even if the mentioned requirements are speaking both for and against a Zero Trust solution, it is obvious that there are many advantages for network operators and users if Zero Trust can be applied for OT environments as well.


Zero Trust Network Access
Zero Trust Exchange
OT Network
SCALANCE LPE + Zscaler App Connector
Zero Trust enabled Application Segments

Combined strength of Siemens and Zscaler

As a result, Siemens is taking the approach that Zero Trust Network Access is a fundamental component of an industrial network following the Defense in Depth strategy supported by Zscaler Zero Trust Exchange. With Zero Trust gateways like the Siemens local processing engine SCALANCE LPE – which runs Zscaler App Connectors in docker container format directly at the cell networks and next to existing cell firewalls – a feasible concept can be established. This enables factories to bring IT and OT closer together with the assurance of Zero Trust connectivity while preventing the bad guys from getting to the OT side. It thereby also enables factories to deprecate VPNs at this layer, reducing cost and complexity, adding agility and reducing risk.

At the end of the day, it is important to understand that IEC 62443 always follows a risk-based approach and there is always a residual risk that needs to be accepted by an asset owner or network operator. It also means that a specific solution may fit for some production networks while others require a different solution. To be compliant to IEC 62443, several factors must fit together – it's necessary to have a security system comprising different technologies but also a security program comprising trainings and organizational measures. Therefore, it is not possible to state that a certain solution is always compliant to IEC 62443, but the solution can support in establishing a compliant security system and program. A suitable approach to demonstrate conformity of the Siemens Zero Trust Solution with IEC 62443 offered as part of the Siemens-Zscaler partnership is described in the following.

Depending on the intended operational environment and intended use, an additional device, Siemens SCALANCE LPE, will be attached to the barrier device protecting the target network cell. It is recommended to use a firewall to protect the network segment to create a specific subnet for the SCALANCE LPE, a kind of micro-DMZ (demilitarized zone). With the Zscaler App Connector hosted on the SCALANCE LPE device, an outbound tunnel connection on port 443 can be established to one of the Zscaler Service Edges. This may be located on-premise or in a cloud infrastructure, depending on the IEC 62443 security assessment.

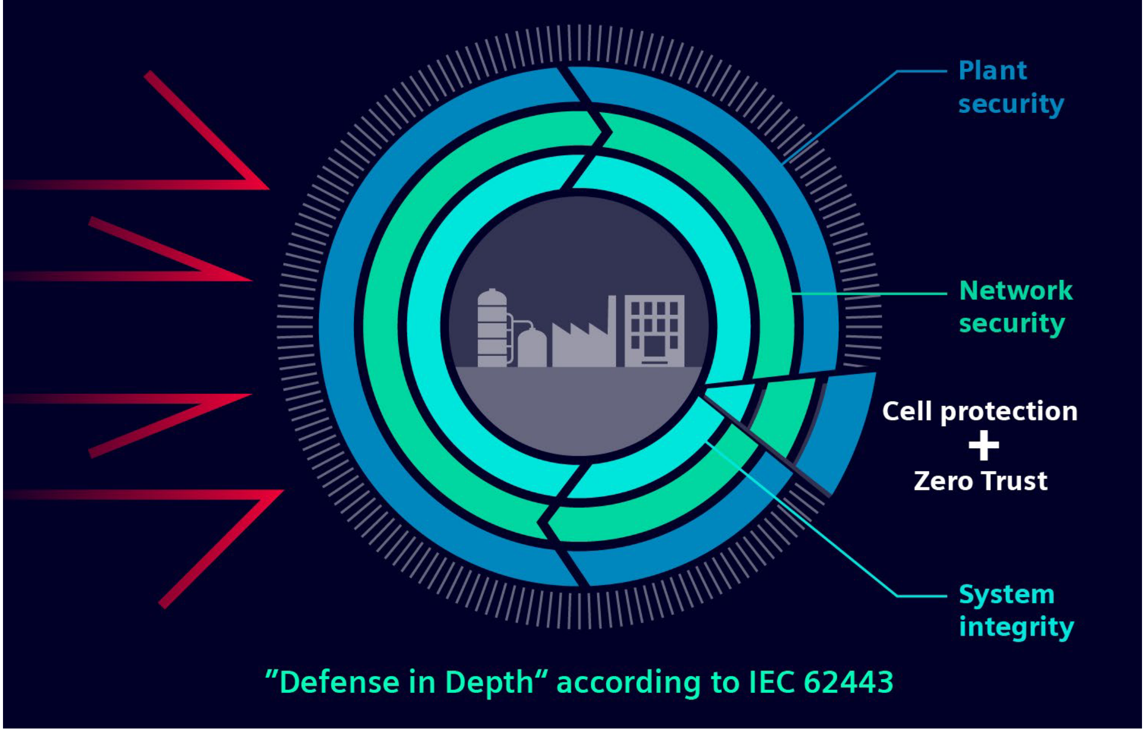
Step 1:
defining access

In a first step, the intended use of the solution needs to be defined to specify the scope and architecture of the Zero Trust solution. As part of this step, it must be defined which users shall have access to the necessary assets to perform their dedicated task. Depending on the potential impact concerning health, safety and environment, the IEC 62443 recommends assigning appropriate user rights, following the principles of least privileges, to perform specific tasks. For critical production environments and segments, it may be necessary to prevent any controlling activities and to authorize only monitoring capabilities. For other areas, it may be allowed to actively control certain functionalities remotely. Moreover, the required strength of authentication needs to be considered in this step, which is often part of a security assessment – the best case multi factor authentification.

To avoid any impact on availability of the production and manufacturing process, critical communication should remain local within the production network.

Step 2:
specifying the environment

In a second step, the intended operational environment for Zscaler Zero Trust Exchange needs to be specified. This means that the circumstances for a Zero Trust network access


Plant security
Network security
Cell protection + Zero Trust
System integrity
”Defense in Depth“ according to IEC 62443

Proven ”Defense in Depth” security enriched by the Zero Trust principles.

must be described. For a simplified consideration, it will be assumed that the target environment follows the recommendations of IEC 62443 and that a classical perimeter-based network concept – comprised of perimeter and network cells – has been established. Additionally, the target security levels must be assessed and all required operational measures maintained. Under this condition, the Zscaler Zero Trust Exchange comprising its infrastructural component called App Connector is considered a separate security zone and added to the target environment. App Connectors are lightweight containers located in front of private applications deployed at the edge of the network cells. They broker security connectivity between an authorized user and a named app with an inside-out connection, which therefore doesn’t expose application to the internet.

Step 3:

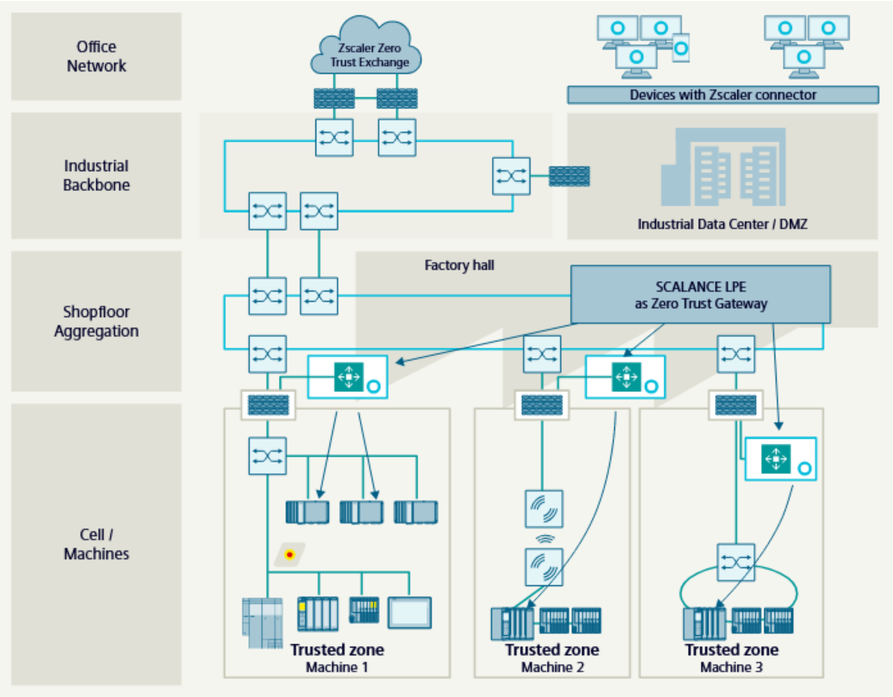
choosing a system concept

In a third and final step, an architectural system concept must be chosen to fulfil the technical requirements of IEC 62443 and to realize the defined demands of the previous steps. To enable compliance with IEC 62443, it is strongly recommended to stick to the classical perimeter-based security concepts for OT. In doing so, the availability of systems and assets can be ensured even if there are peak loads, misconfigurations or security issues in other network segments, such as the backbone network. The remote access to a specific application running in one of the identified target network cells will then be realized by Zscaler Zero Trust Exchange.

As stated above, the Zscaler Zero Trust Exchange will be considered a separate zone, meaning that there is still the requirement of controlling and restricting the data flow to the target application hosted in the connected network cell. This can be achieved by some specific inbound firewall rules controlling the traffic between the Zscaler App Connector and the target connector. With this approach, it is possible to segment networks according to security levels and protect zone boundaries to restrict data flow at a zone boundary while granting access to specific applications on demand. Depending on the results of the risk assessment, it would also be possible to isolate mission critical network segments and to prevent lateral movement between the connected network segments.

To sum up, current objective is not to replace existing perimeter-based security concepts, established by firewall or by other means based on overlay technologies, but rather to enrich it with Zero Trust principles and to evolve it over the coming years.

In the following, we outline a few key requirements of the IEC 62443 and show how the Siemens Zscaler partnership for Zero Trust access can support compliance with the standard.



SR1.13: All about access

Monitoring and controlling all access to the control system via untrusted networks

Zscaler Private Access (ZPA) only provides access via untrusted networks if the user has provided authentication with the Identity Provider (IdP).
The IdP can be completely managed by the customer or any outsourced entity. The customer's IdP is responsible for authentication and authorization of users that request access to devices connected via ZPA. Siemens and Zscaler do not gain any knowledge of the users or devices inside a customer's network. As part of the authentication flow, the IdP grants access tokens that are used to define access policies for least privileged access.

SR1.13RE1: Approval required

Denying access requests via untrusted networks unless approved by an assigned role

ZPA will deny access via untrusted networks by default if the user has not been authenticated with the IdP. Depending on the configuration and the assigned user rights, access will be granted to specific devices to carry out defined tasks with specified applications. It is also possible to define trusted networks within the policies and provide authenticated users access from those locations only.

SR4.1: High confidentiality

Protecting the confidentiality of information at rest, transit and remote access sessions on an untrusted network

By default, with Zscaler Zero Trust Network Access, traffic from Zscaler Client Connectors and App Connectors is encrypted using mutually authenticated DTLS or TLS tunnels to the ZPA Public Service Edge or ZPA Private Service Edge. For clientless, browser-based access, the web browser should support TLS 1.2. On demand and end-to-end data streams between Client Connector and App Connector can be encrypted with a double-encryption micro tunnel. In doing so, the transmission of unencrypted protocols can be additionally secured when the traffic flows through the Zscaler Service Edges.

SR5.1: Clear separation

Segmenting control and non-control system networks

Zscaler App Connectors are deployed in segmented network cells secured by barrier devices such as SCALANCE S firewalls. With the local processing engine SCALANCE LPE placed in a separate subnet created by the firewall, a micro-DMZ is created for Zero Trust Network

Access. Thus, App Connectors deployed on the Siemens SCALANCE LPE are located close to internal applications and the control system. App Connectors never communicate with each other and do not accept inbound connections.

To provide users access to internal applications or control systems, App Connectors only require an outbound connection to reach ZPA Public Service Edges on the internet or ZPA Private Service Edges hosted within the customer data center. Using a key pair (i.e., a provisioning key and a corresponding TLS client certificate), the App Connector and the ZPA cloud verify each other as part of enrollment. Once an App Connector is enrolled, the TLS client certificate allows it to maintain its authentication with the nearest ZPA Public Service Edge or ZPA Private Service Edge, which provides the App Connector with its configuration to perform its operational tasks.

SR5.2: Zone Boundary Protection

Monitoring and controlling communications at zone boundaries and enforcing the compartmentalization defined in the risk-based zones and conduits model

As the App Connector is hosted on the SCALANCE LPE device within a micro-DMZ segment, the traffic from the App Connector to the local application is restricted. With user-defined firewall rules, as provided by SCALANCE S, for instance, it becomes possible to load a user-specific set of rules by simply sending an input to the firewall appliance. The signal can originate by physical key switch, a PLC or by a user authentication at the firewall. Whether such additional firewall rules are required will result from the IEC 62443 assessment, which should have been conducted beforehand.

SR5.3: Secure connectivity

Preventing general purpose, person-to-person messages from being received from external sources

App Connectors deployed on the Siemens SCALANCE LPE are located close to internal applications and the control system. App Connectors never communicate with each other and do not accept inbound connections. To provide users access to internal applications or control systems, App Connectors only require an outbound connection to reach ZPA Public Service Edges on the internet or ZPA Private Service Edges hosted within the customer data center.

ZPA decouples applications from the physical network, providing seamless and secure connectivity to private internal applications or control systems deployed at the field level.

Zero Trust, maximum impact

Having these advantages in mind, a holistic and transparent Zero Trust Network Access solution for complete enterprises comprising IT and OT networks can be established – without exposing productivity to a higher risk. With the concept of an enriched OT security concept, data flows can be controlled on a task-to-task basis and access to OT can be as easier and simpler than ever before. Please keep in mind that possible national regulations for critical infrastructure are not considered.

Published by
Siemens AG

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

For the U.S. published by
Siemens Industry Inc.

100 Technology Drive
Alpharetta, GA 30005
United States

Article number:
6ZB5530-2FC02-0BA1
Produced in Germany

Subject to changes and errors. The information provided in this brochure contains descriptions or performance characteristics 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. The desired performance characteristics are only binding if expressly agreed in the 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, the use of which by third parties for their own purposes may violate the rights of the owners.

Support:
Please direct any questions in connection with this White Paper to your Siemens contact person at your representative/sales office.

Security information
Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks. 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. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be implemented, please visit **siemens.com/industrialsecurity**. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under **siemens.com/cert.**