Industrial DMZ Infrastructure
Cybersecurity in OT environments requires automation expertise

Operative challenges

• To protect against cyber attacks, the international security standard IEC 62443 recommends a deeply tiered defense, including network segmentation

• In the corresponding "Zones & Conduits" model, the IEC 62443 standard recommends not to enable direct communication between IT and OT

• The requirements of operational technology (OT) differ greatly from those of office IT, e.g. long asset lifecycles with discontinued systems, high system heterogeneity, plant availability as main objective

• The technical implementation of security measures cannot be transmitted 1:1, experience in operational environment is necessary

• IT staff needs support from security experts with automation know-how

Digitalization without security is not possible – but the specific requirements of the automation environment have to be considered carefully.

Required solution

- Combined expertise in automation, digitalization and security
- Turnkey comprehensive security concepts for automation environment
- Digitalization of industry while keeping high availability, reliability and security
Secure data exchange between IT and OT with Industrial DMZ Infrastructure

Solution

Industrial DMZ Infrastructure is a ready-to-run concept for the segmentation of IT and OT networks with integrated security features. Thanks to the combined know-how of Siemens experts in the fields of automation, digitalization and cybersecurity, this single-source solution is optimized for use in production and meets the highest requirements in terms of availability and security.

How does it work?

- The concept is based on the principle of the demilitarized zone (DMZ) with front and back firewalls to protect the OT systems from unauthorized access.
- Hardware, software and services for network security and system integrity are already integrated, serving two of the three layers of the Defense in Depth concept.
- The solution is implemented on the proven hyper-convergent IT platform Industrial Automation DataCenter, allowing high performance computing with virtualization.
- The holistic approach covers consulting, configuration and appropriate support services throughout the entire life cycle.
Virtualized DMZ with state-of-the-art technology

IT/OT network segmentation
- DMZ (demilitarized zone) with redundant front and back firewalls protects the OT systems from unauthorized access from outside.

State-of-the-art
- “Next Generation” firewalls go beyond protocols and port inspection of classic firewalls and facilitate data analysis at the application level (layer 7).

Virtualized DMZ
- The services in the DMZ, e.g., remote access, file exchange, and active directory, are made available as virtual machines on a separate high-performance virtualization host.

Zero trust
- The DMZ itself is based on the zero-trust concept, therefore the communication between the virtual machines within the DMZ is effectively prevented and only takes place via the firewalls.
Siemens holistic security concept: Defense in Depth based on IEC 62443
Industrial Cybersecurity Services: End-to-end approach

**Plant Security Services**
- Security Assessments
- Scanning Services
- Industrial Security Consulting
- Security Awareness Training

**Network Security Services**
- Industrial Next Generation Firewall
- Industrial DMZ Infrastructure
- Industrial Anomaly Detection

**System Integrity Services**
- Endpoint Protection
- Industrial Vulnerability Manager
- Patch Management
- SIMATIC DCS / SCADA Infrastructure
- SIMATIC Security Service Packages

- Transparency about the current security status
- Increased security level by closing security gaps
- Long-term protection through continuous security management
Industrial Cybersecurity Services can be integrated into Industrial DMZ Infrastructure
Implementation on the hyper-convergent IT platform
Industrial Automation DataCenter

The Industrial Automation DataCenter is an individually configured data center, developed for all IT requirements in production. It includes all important core components of a data center, such as high performance computing (with high availability), IT/OT networks, back-up and disaster recovery, process data archiving, uninterruptable power supply and IEC 62443 compliant security architecture.

Pre-configured and pre-tested HW/SW components

1. Front Firewall
2. Industrial DMZ
3. Back Firewall
4. IT Networking
5. Computing
6. Backup & Disaster Recovery
7. Process Historian
8. OT Networking
9. Uninterruptable Power Supply
We are the automation experts

We drive digitalization

We understand industrial security

We have specific industry know-how

We offer state-of-the-art technology and end-to-end services from a single source

“We make sure that you can focus on your core business.”
Why should you choose Industrial DMZ Infrastructure?

- IT/OT network segmentation based on IEC 62443
- Defense in depth with security features out of the box
- Hyper-convergent IT infrastructure for high performance computing
Let us know if there is anything we can support you with!
Disclaimer

© Siemens 2022

Subject to changes and errors. The information given in this document only contains general descriptions and/or performance features which may not always specifically reflect those described, or which may undergo modification in the course of further development of the products. The requested performance features are binding only when they are expressly agreed upon in the concluded contract.

All product designations, product names, etc. may contain trademarks or other rights of Siemens, its affiliated companies or third parties. Their unauthorized use may infringe the rights of the respective owner.
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 https://www.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 https://www.siemens.com/industrialsecurity.