Industrial DMZ Infrastructure

Secure data exchange between IT and OT

SIEMENS

Cybersecurity in OT environments requires automation expertise

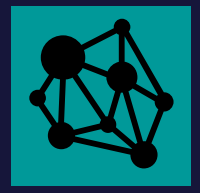
Operative challenges

- 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

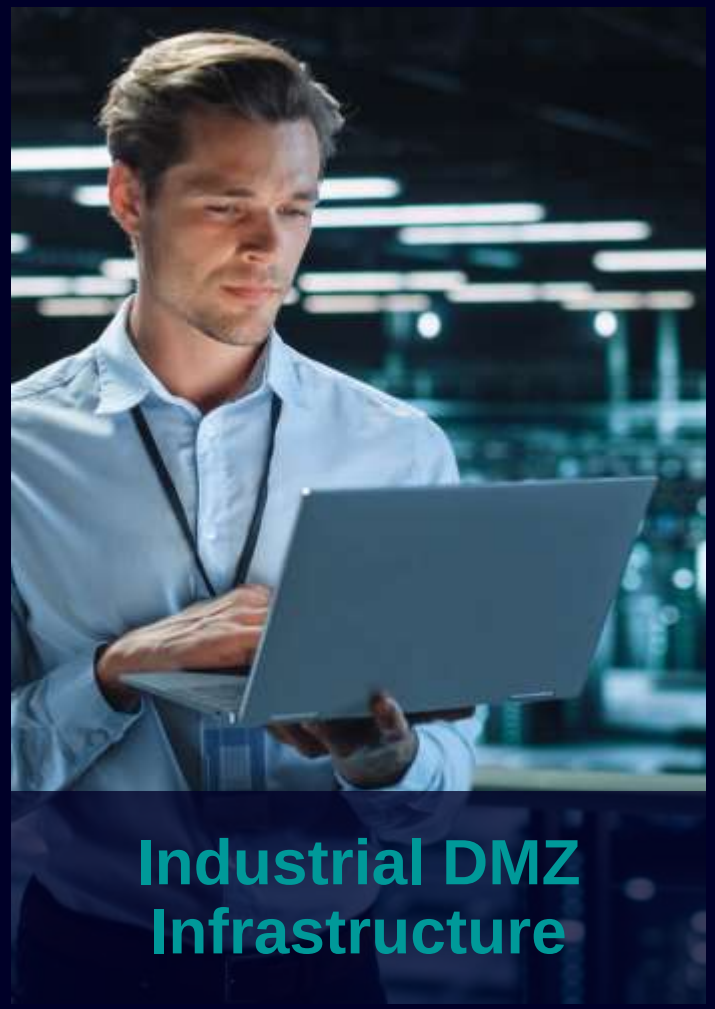


Turnkey comprehensive security concepts for automation environment

Digitalization of industry while keeping high availability, reliability and security

SIEMENS

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.

SIEMENS

Virtualized DMZ with state-of-the-art technology

IT/OT network segmentation

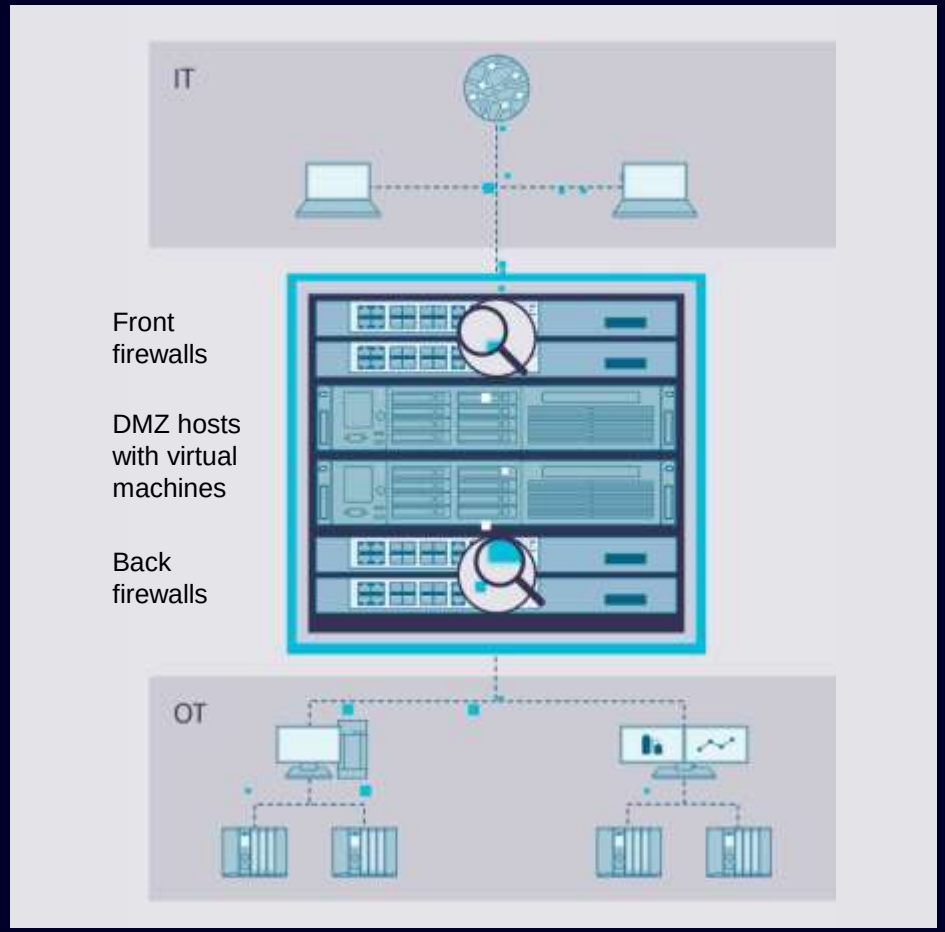
- DMZ (demilitarized zone) with redundant front and back firewalls protects the OT systems from unauthorized access from outside.

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 are made available as virtual machines on a separate high-performance virtualization host:
  - **Data Exchange Server:** data delivery between IT/OT networks
  - **Jump Host:** remote access to DMZ host and OT network
  - **Domain Controller:** centralized user and computer management; authentication and security
  - **Network Monitor Server:** IT/OT monitoring based on PRTG
  - **Management:** enable centralized network management
  - **Domain Name System:** enables use of domain names
  - **Endpoint Protection:** antivirus and allowlisting
  - **Information Server:** web-based reporting system
  - **Update Server:** WSUS patch management



SIEMENS

Cybersecurity Management Tools
Network Monitor Server: IT/OT Asset Monitoring based on PRTG

What is it about?

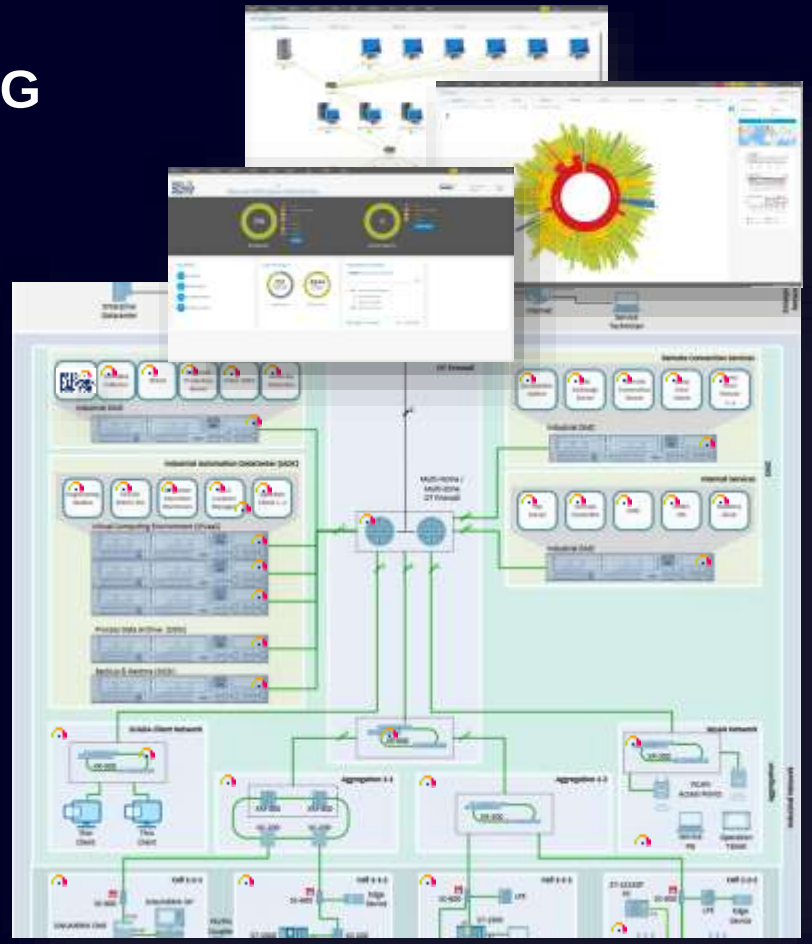
Your IT/OT infrastructure must function reliably to ensure the operational continuity of the entire system. Therefore, it is important to identify problems at an early stage before they cause a failure.

With IT/OT Asset Monitoring, we provide the perfect solution to monitor all critical hardware and software components of your OT environment.

This enables you to prevent downtime and thus boost the availability and reliability of your entire production.

How does it work?

- Asset monitoring by using standard protocols like WMI, SNMP, SSH, OPC UA, HTTPS and many more (an asset can be a hardware or software component).
- Get notified via email, SMS/pager, OPC UA.
- Create new value by combining acquired information, e.g. health status of all hard disks.
- Share all your data with your OT environment for monitoring and alerting purpose.
- Monitor many production sites even across continental borders. Ask our experts!
- Get creative visualizing your IT/OT environment with the map functionality of PRTG.



Deliverables

IT/OT Asset Monitoring based on PRTG

Software licenses and services

- Available in batches of 500, 1.000, 2000, 5.000, 10.000 asset sensors
- Including a half-day start-up consulting for commissioning and implementation
- Technical support for 3 or 5 years
- Software maintenance for 3 or 5 years
- Implementation and commissioning services (optional)

SIEMENS

Siemens holistic security concept: Defense in Depth based on IEC 62443

Security threats demand action

Defense in Depth

based on IEC 62443

- Plant Security
- Network Security
- System Integrity
- Industrial Cybersecurity Services

SIEMENS

Industrial Cybersecurity Services: End-to-end approach

Plant Security Services

- Security Assessments
- Industrial Security Consulting
- Cybersecurity Trainings
- Remote Industrial Operations Services

Transparency about the current security status

Network Security Services

- Industrial Next Generation Firewall
- Industrial DMZ Infrastructure
- Remote Platform Software as a Service

Increased security level by closing security gaps

System Integrity Services

- Endpoint Protection
- Vilocify Vulnerability Services
- Patch Management
- Backup and Restore

Long-term protection through continuous security management

SIEMENS

Industrial Cybersecurity Services @ Industrial DMZ Infrastructure

SIEMENS

Why not profiting from the industrial digitalization age and get Siemens on board for your IT/OT infrastructure?

Managed IT/OT Infrastructure

- includes a ready-to-run high-available IT infrastructure for OT environments.
- meets sustainability goals and the latest cybersecurity requirements.
- ensures operational continuity through remote management and monitoring by IT/OT experts.

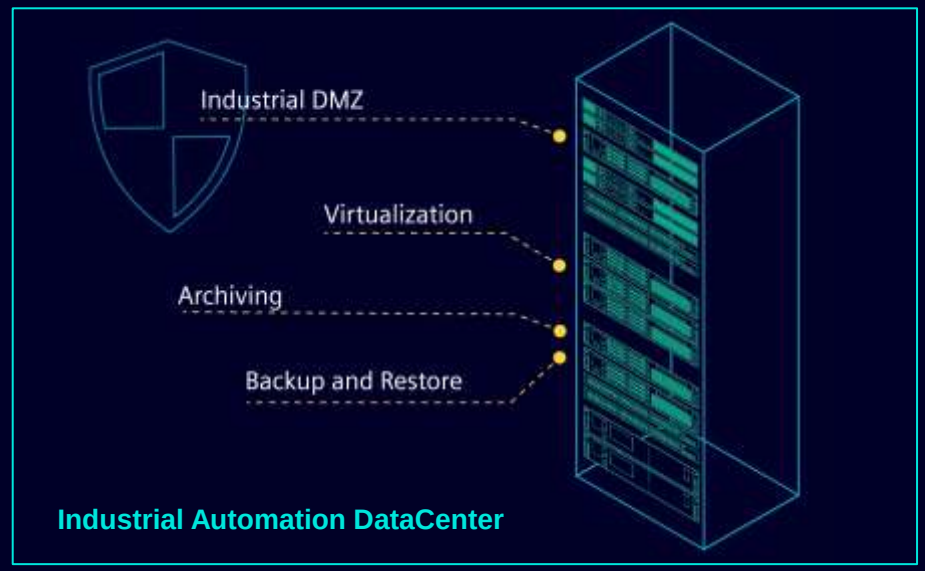
➢ **bridges the gap between IT and OT.**

The perfect symbiosis of hardware, software and services

Secure data exchange between IT and OT based on IEC 62443 with industrial DMZ infrastructure

Future-proof modernization of control systems with a pre-configured virtualization platform

Pre-configured IT infrastructure for optimized data handling:
- Archiving
- Backup and Restore



+

Remote monitoring and management of your IT/OT infrastructure by IT/OT experts through the entire life cycle

SIEMENS

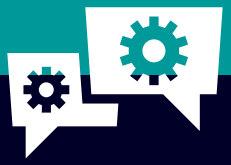
Siemens as reliable partner for IT infrastructure in OT environments

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."

SIEMENS

Why should you choose Industrial DMZ Infrastructure?

IT/OT network segmentation based on **IEC 62443**

Defense in depth with integrated security features

Hyper-convergent IT infrastructure
for high performance computing

SIEMENS

Let us know if there is anything we can support you with!

You want to find out more?

Here you can find more information:

siemens.com/idmz

or contact the Siemens partner near you

Siemens Contact Database

SIEMENS

Disclaimer

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.

SIEMENS

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 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

SIEMENS