infinigate
spark your growth

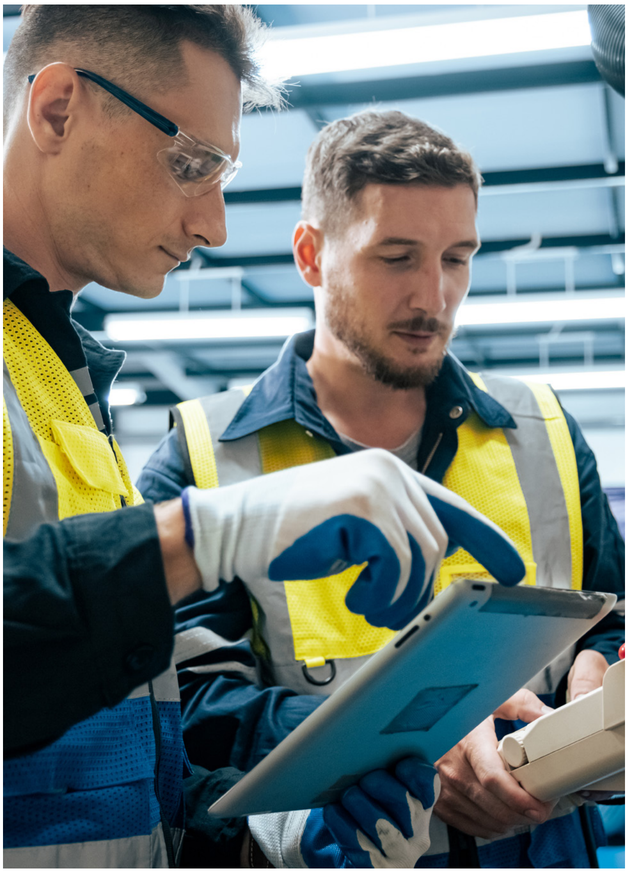
OT security

Protecting important infrastructure, work environments and people.

OT security: keep your automation and control systems safe

OT security stands for 'Operational Technology' security and refers to practices and technology that aim to protect industrial automation and control system (ICS), and other critical infrastructure from cyber threats.

Unlike IT security, which focuses on computer networks and data, OT security focuses on the security of physical devices, machines, plants and processes. As many of these systems were not developed with direct internet access in mind and are often based on older operating systems (Microsoft Windows XP, Microsoft Windows 7, etc.), they can be vulnerable to cyber attacks.



Cybersecurity leadership

1 OT is used in manufacturing to automate and control production processes, monitor machines and plants and guarantee product quality.

2 In the energy sector, OT controls and monitors power plants, power grids and other energy infrastructure for generating, transmitting and distributing electricity and other energy sources.

3 In the water and wastewater industry, OT is used to control and monitor water treatment plants, pumping stations and distribution systems to ensure a reliable supply of water and disposal of wastewater.

4 In the transport sector, OT controls and monitors traffic signals, rail and road traffic systems, airports and other transport infrastructure to ensure people and goods are transported safely and effectively.

5 OT is used in public health services to control and monitor medical devices, patient monitoring systems and hospital infrastructure, to improve patient care and safety.

Available OT infrastructure is essential for the following reasons:

1. Operational disruptions and production downtime involve enormous financial risks, such as loss of sales, repair costs and damage company reputation.

2. OT system failures can jeopardise the physical safety of employees, the general public and the environment.

3. In addition to the physical effects, cyberattacks on OT systems can lead to the theft of sensitive data and sabotaged processes. This can generate long-term security issues and competitive disadvantages for affected companies.

The NIS2 directive, applicable in Europe from October 2024, and the Cybersecurity Resilience Act (CRA) play a particularly important part in OT security by significantly increasing security requirements and standards for companies classed as essential and important, such as construction engineering companies and service providers.

The risk management measures required by law, such as risk analysis, security policies and strong security in the supply chain, also apply to OT security.

Do you have questions about NIS2 and CRA?

Download
the whitepaper.

OT Security:
Systematic implementation

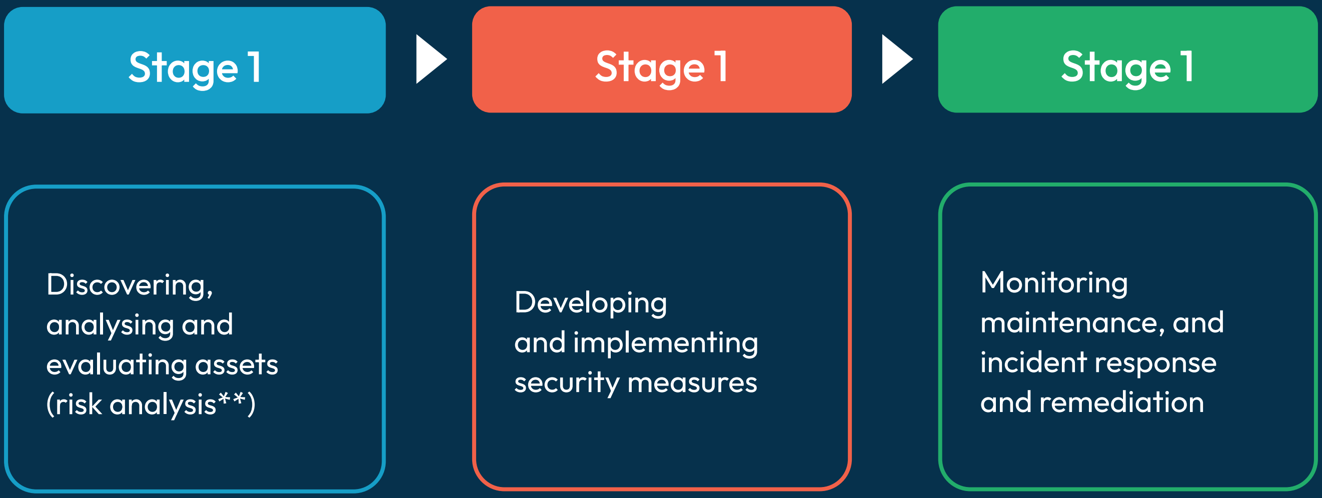
The ISA/IEC 62443 is an international series of standards developed specifically for the security of industrial automation and control systems.

It provides a comprehensive framework for implementing OT security measures and procedures. It defines clear security standards and best practices for planning, implementing and managing OT security measures.

It defines a systematic approach to implementing security measures that helps all stakeholders effectively improve, monitor and continuously maintain their OT systems.

At the same time, this system helps to fulfil the NIS2 and CRA legal requirements.

The 3 stages of OT security*



Stage 1

Discovering, analysing and evaluating assets (risk analysis**)

Stage 1

Developing and implementing security measures

Stage 1

Monitoring maintenance, and incident response and remediation

*see also ISA/IEC 62443 2-1, ** see also NIS 2 article 21

The cornerstones of OT security

The following elements are required to comprehensively implement OT risk management measures. They are essential for taking the ‘deep defence’ approach to OT security. ‘deep defence’ means implementing appropriate security levels to protect a production facility from threats. Combining a series of countermeasures reduces the risk of a successful attack. This approach includes physical, logical and process-related security measures, which create a robust security architecture.

Risk analysis, evaluations and reviews	IT/OT asset discovery, management and threat detection (selection, implementation and operation)	Endpoint protection and checks (AV, host IDS/EDR, data protection, USB checks)	Monitoring & threat intelligence
Employee training and awareness	Secure remote access	Vulnerability management, configuration hygiene & patch management	Backups, incident response, recovery and business continuity planning (BCP)
Network architecture and segmentation (IT/OT)	Identity and access management and control	Supply chain security (risk mitigation with regard to software Bill of Material (BOM), OEMs and service providers)	Audits, pen tests and continuous improvement process
IT/OT security corporate policy andorganisation			

Examples of five-stage implementation of OT security principles

1.

Network architecture and segmentation (IT/OT)

— IT-OT-DMZ macro segmentation using two layers of physical firewalls.

— Defining a restrictive data flow from OT to IT, not the other way around.

— Continuing network micro-segmentation based on zones and cables.

2.

Asset inventory and checks**

— The objective is to be aware of ALL assets requiring protection in the network. This is absolutely essential, especially in production networks that have grown over time.

— Asset management is a core component of modern IACS/OT networks – and is required by NIS2!

— Even if every single asset has not been recorded, any high number is a good starting point.

— Asset management must be up to date. If it is out of date or doesn't exist at all, it must be started promptly!

3.

Incident response planning

— The ability to respond to an incident in an organised manner using a process plan.

— Key points include, but are not limited to:

- People's safety
- List organisations that need to be contacted for assistance?
- List authorities who should be notified?
- Fast recovery of PLC functionality
- Getting production and machinery back into operation and production running again

4.

Backup and recovery

— Key points include, but are not limited to:

- Location of backups (internal/external)
- Completeness of backups in relation to assets
- Asset recovery time
- Test backup recovery in advance
- Documented recovery instructions

** see also NIS 2 article 21

5.

Continuous vulnerability management

— Vulnerability management in ICS/OT works differently from IT.

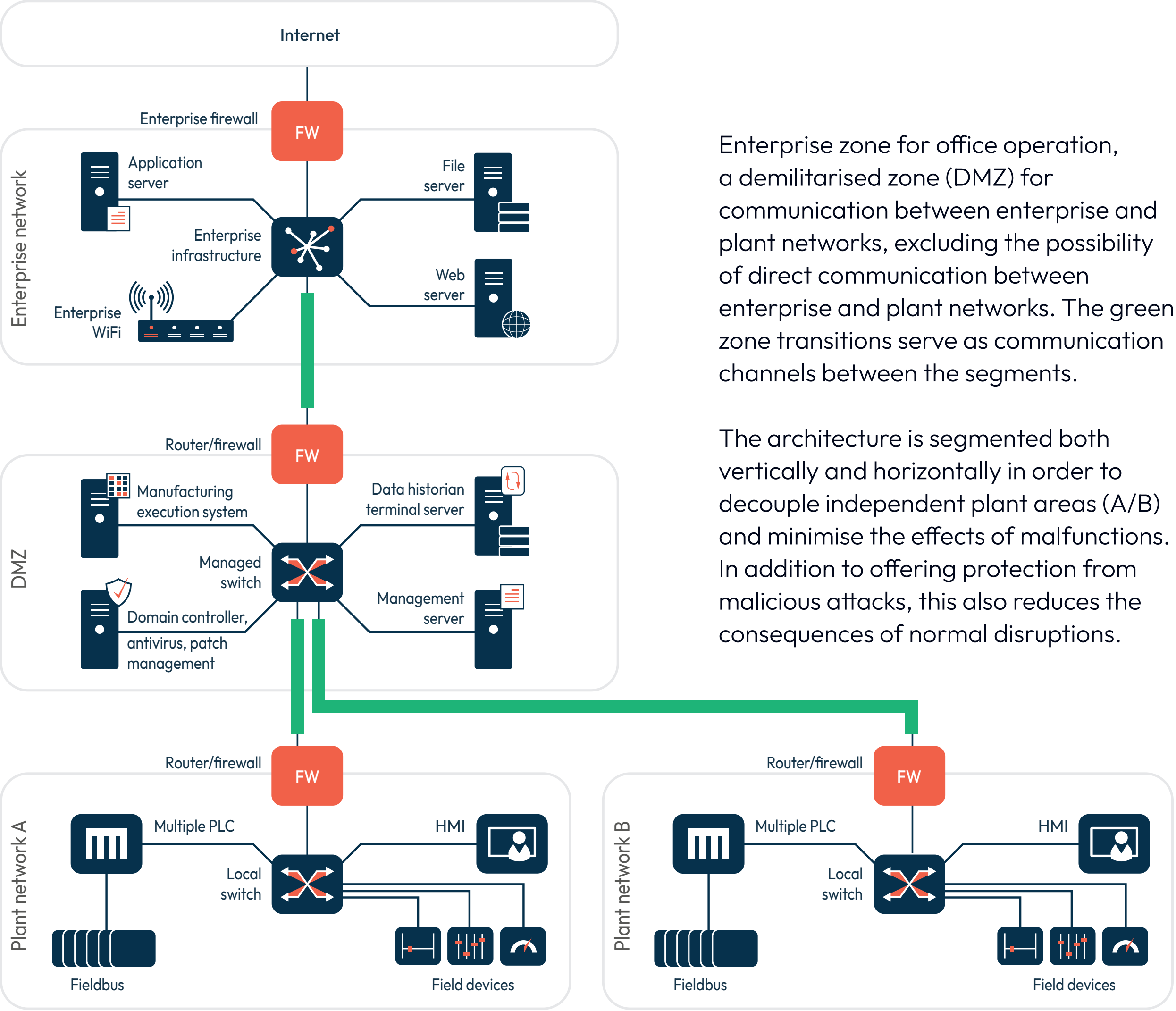
— Inventory is mandatory (see no. 2 on the previous page)

— Key points include, but are not limited to:

- Identifying current vulnerabilities
- Manufacturer classification of the risk
- Risk analysis with regard to threats and consequences

Risk mitigation through network segmentation

The following figure shows a network architecture that is divided into four zones:



Enterprise zone for office operation, a demilitarised zone (DMZ) for communication between enterprise and plant networks, excluding the possibility of direct communication between enterprise and plant networks. The green zone transitions serve as communication channels between the segments.

The architecture is segmented both vertically and horizontally in order to decouple independent plant areas (A/B) and minimise the effects of malfunctions. In addition to offering protection from malicious attacks, this also reduces the consequences of normal disruptions.

A comprehensive approach to OT security at every stage

As a leading added value distributor of OT security, Infinigate provides a comprehensive approach and professional, specialist services, expert consultancy and supporting services such as OT engineering and financing services.

	Network architecture & segmentation	IT/OT asset discovery & threat detection	Endpoint protection	Monitoring & threat intelligence	Secure remote access	Vulnerability management, patch management	Incident response	Identity & access management and control	Supply chain security
ARMIS		✓		✓	✓	✓	✓		
Barracuda	✓				✓	✓	✓	✓	
CHECK POINT	✓	✓	✓	✓	✓		✓		✓
FORTINET	✓	✓	✓	✓	✓	✓	✓	✓	✓
HPE aruba networking	✓	✓			✓	✓		✓	
kaspersky	✓	✓	✓	✓		✓	✓		✓
macmon intelligent einfach BELDEN	✓	✓			✓			✓	
SOPHOS	✓		✓	✓	✓			✓	
THALES Building a future we can all trust								✓	
txOne networks	✓	✓	✓	✓	✓	✓	✓		✓

OT service portfolio

Technical services

Pre-sales consultation

Our experts will be glad to answer your technical or architectural questions and support you right at your customer's premises.

Demo/PoC support

We can provide the necessary test devices/licences for demo and evaluation purposes. If desired, we also support longer test periods (PoC).

Post-sales support

We are able to relieve your technical department by providing fast support for solutions purchased from us for the majority of our portfolio.

Direct end customer support

If desired, we can provide support at customer's premises, keeping you in the loop and ensuring a high level of customer satisfaction.

Installation & configuration

We offer support to ensure installation and configuration of new solutions goes smoothly, or we can take on these tasks entirely.

Config review/system optimisation

You are using security solutions from Infinigate. Our specialists will help you check the configuration and further optimise it.

Training services

Certification training

We can train you employees the necessary certifications so you can benefit from partner programmes.

Sales

In addition to technical training, we regularly organise sales training courses and webinars on the latest IT/OT security topics.

Technical workshops

If practical knowledge is more important to you than certifications, our technical workshops offer the perfect format for your technicians to develop their knowledge.

Sales & marketing services

Telesales/lead generation

Our experts will be glad to answer your questions. We can generate end customer leads for you on a campaign-related or permanent basis or offer support with customer acquisition for events.bination with one of our manufacturers

Marketing campaigns

We will help define and implement a lead to cash process tailored to your needs.

Renewal support process

We can arrange a well-coordinated recurring revenue process. You will receive custom renewal offers based on the current status and successor SKUs if the initial SKU is no longer available.

Events

We support your marketing team in organising and coordinating the manufacturers involved. We also have an extensive network of suitable speakers on various topics.

Distribution services

Delivery & logistics

From direct delivery to your customers to our private labelling service, where we deliver to the end customer directly on your behalf. Thanks to our high stock availability, we also offer same-day dispatch for many products.

Logistics & export rollout services

For larger rollouts, we can store goods for you to secure supply chains and availability. We also offer international direct deliveries (see Financial Services)..

Configuration rollout services

Have hardware preconfigured on request. We can handle OS and firmware changes, installation of extensions and much more, which is often not offered ex works by the manufacturer.

Advanced hardware replacement (24X7X365)

We offer extended project-based replacement SLAs. We can also enter into international SLAs through local warehousing.

Automate your processes

We provide price lists and product information in various formats and through online portals. There is also the option to connect to your ERP systems using APIs if required.

Partner World and shop

The Infinigate Partner World is a platform on which you as a partner can conveniently organise and manage your business with us. You can order products from selected manufacturers directly from our store.

Finance services channel

Credit limits and project financing

From extending a payment term, increasing your credit limit on a project-by-project or temporary basis, to open and undisclosed assignment. These tools give you maximum flexibility in your business.

Settlement in foreign currency

Avoid currency risks or unnecessary surcharges along the entire sales chain from the end customer to resellers, distributors and manufacturers.

Pre-financing of multi-year orders

Secure the manufacturer's top conditions for multi-year orders and/or grant your customers the required payment periods (annually/quarterly).

International business

With our tax expertise, we can offer support with international transactions, such as direct deliveries within the EU or to non-EU countries. If desired, we can also take care of the customs preparations and the embargo check for you.

About the Infinigate Group

The Infinigate Group, the leading technology platform and trusted advisor in Cybersecurity, Cloud & Network Infrastructure covers over 100 countries. In the 2023-2024 financial year the Infinigate Group revenue reached 2.3B€. Our focus and deep technical expertise on cybersecurity, secure networks and secure cloud for SMB and enterprise set us apart. Our 1,250 employees provide locally tailored services complementing a robust central supply chain, sparking growth for our partners, MSSPs and vendors.

Infinigate Holding AG
Grundstraße 14, CH-6343 Rotkreuz
Switzerland

info@infinigate.com
www.infinigate.com

infinigate
spark your growth