OTD BİLİŞİM
GLOBAL VAD

advenica
Swedish cybersecurity
at your service

Secure connectivity principles for Operational Technology (OT)_

The National Cyber Security Centre (NCSC-UK) has released eight Secure Connectivity Principles for Operational Technology (OT), in collaboration with international partners. Advenica has been a trusted cybersecurity provider and applied these principles for decades. Learn more about how we apply these principles and help organisations design, secure, and manage connectivity in OT.

The principles we cover in this article

- Balance the risks and opportunities
- Limit the exposure of your connectivity
- Centralise and standardise network connections
- Use standardised and secure protocols
- Harden your OT boundary
- Limit the impact of compromise
- Ensure all connectivity is logged and monitored
- Establish an isolation plan

Balance the risks and opportunities

• Before you start implementation, it's recommended to formulate a business plan that is auditable and apply a risk management framework such as ISO 27000, IEC 62443 or similar.

• Goal Structuring Notation (GSN) is an approach that Advenica often use when building security arguments for complex systems. By defining your security targets in a GSN-tree you get a good overview and can clearly motivate certain security measures, both technical and non-technical.

• To manage your supply chain, ensure that the devices you use are secure by design and that they can easily be upgraded without disrupting your business.

Limit the exposure of your connectivity

Reduce time of exposure

Your equipment might be in a remote location while you need to do some maintenance that you can't automate. The Advenica Remote Access Device provides temporary connectivity with two factor authentication. The device can be used as a remote KVM, a terminal or provide IP-based access; all through an encrypted remote access tunnel.

Remove inbound port exposure

All external connections with the OT network should be initiated from the inside. When the inbound connections are protected using Data Diodes, the Data Diode Engine is configured to initiate the communication with external assets.

Manage obsolescence risks

Obsolete devices pose an increasing risk, but they might not be possible to replace right away for operational reasons. The Advenica DD500E Data Diode is a cost effective way to isolate such devices while still maintaining connectivity.

Manage unique connectivity comes with risk

Remote connections between different production sites might be needed, but this also introduces risk. Public internet links carry higher exposure than private fiber. Advenica provides hardware based IP encryption systems, designed for tactical and strategic defence operations. These devices minimise external attack vectors by default and are designed to be connected directly to the internet. The encryption devices maintain an internal network between the sites with enough security to protect a nation.

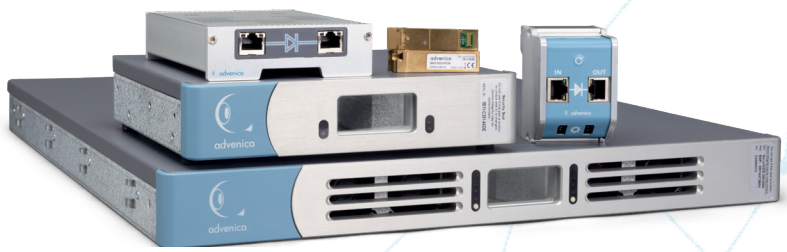
Centralise and standardise network connections

• Your OT remote connectivity should be flexible, repeatable and categorized.

• File Security Screeneris a high-security file import solution combining unidirectional data diode technology with malware scanning.

• ZoneGuard can be adapted to validate and filter any protocol for data transfers. ZoneGuard can communicate in both directions, but for uni-directional cases it can be combined with a data diode such as the DD1000i.

• These solutions can be configured to be the single point of entry for your OT network.



Use standardised and secure protocols

• Security might be a tradeoff between confidentiality, integrity and availability (CIA).

• ZoneGuard has support for TLS based communication, but the protocol break enables its flexible services to validate the data against pre-defined schemas.

• The Advenica Customised Solutions team will help you add or modify Zoneguard or Data Diode services to fit your protocol needs.

Want guidance or help finding the right solution for your organisation? We are at your service.

Harden your OT boundary

• Obsolete assets and weak security controls within the OT environment make hardening of the system boundaries critical.

• Segmenting the networks with hardware based Data Diodes and Cross Domain Solutions decreases these risks.

Limit the impact of compromise

Operational hygiene means that you shouldn't connect laptops used in the office network to your OT network. SecuriRAM allows you to move files to and from your OT workstation without bringing malware by mistake.

Segmentation

A strategy of segmenting the OT network into separate zones limits the room for lateral movement. While protecting the external boundaries of the OT network might require high performance Data Diodes like the DDSFX-10G, cost effective variants like the DD500E could be deployed to protect a single machine or a group of machines.

Separation of duties

It's sensitive to import files or data to an OT network, exporting data to your business systems could often be done with a single Data Diode. The Data Diode Engine proxy software helps you to convert your bi-directional protocol to a uni-directional UDP data stream. The UDP stream is sent over the Data Diode before it's converted back to the original protocol. The Data Diode Services that does this are customisable for your needs.

Browse down

The management interfaces of the ZoneGuard and the Data Diode Engine are secured by certificates. These should only be handled by privileged access workstations according to your PAWs policy.

Boundary Controls

The outer end-point of the Data Diode Engine is located in a DMZ that could be protected by a firewall for additional layers of security.

Ensure all connectivity is logged and monitored

• Monitoring is your last line of defence for secure connectivity.

• The Advenica Data Diodes could easily be used to export logs to an external SOC while preventing attacks on the SOC from spreading back to the monitored OT network.

Establish an isolation plan

• With the help of the GSN tree, you should be able to analyse what is needed to keep your systems running should there be a breach to one of your network segments. This might involve improvements to your physical production process to facilitate resilience.

• A network kill switch could be prepared by placing the Remote Access Device in strategic locations.

• By utilising the built-in LTE connection for redundant connectivity, you can maintain control also during a severe attack on your infrastructure.

Contact us to learn more about how Advenica can help your organisation adhere to the secure connectivity principles for Operational Technology (OT).

Advenica provides cybersecurity solutions within encryption and network segmentation with the highest level of EU-and national approvals. We were founded in 1993 and are based in Malmö, Sweden, where most of our products are designed, developed, and manufactured. Advenica specialises in the sectors of defence, authorities, infrastructure, and industry. With decades of experience working with Sweden's national security, Advenica is known for delivering cybersecurity with exceptional service.

Read more at advenica.com

advenica
Swedish cybersecurity
at your service

OTD BİLİŞİM
GLOBAL VAD