Securing information flows in an IT/OT environment

The need to connect IT and OT has grown with the digitalisation of production processes. But how do you secure this information flow and avoid exposing your systems to cyberattacks?

Challenge

Secure information flow in an IT/OT environment

It has become increasingly important to be able to connect IT and OT. There is also the need to securely manage the systems and to retrieve system events from both IT och OT environments. This need has grown with the digitalisation of production processes and society as a whole. IT and OT are therefore connected, and similar technology is often used in IT and OT. The different needs in IT and OT can easily lead to challenging conflicts

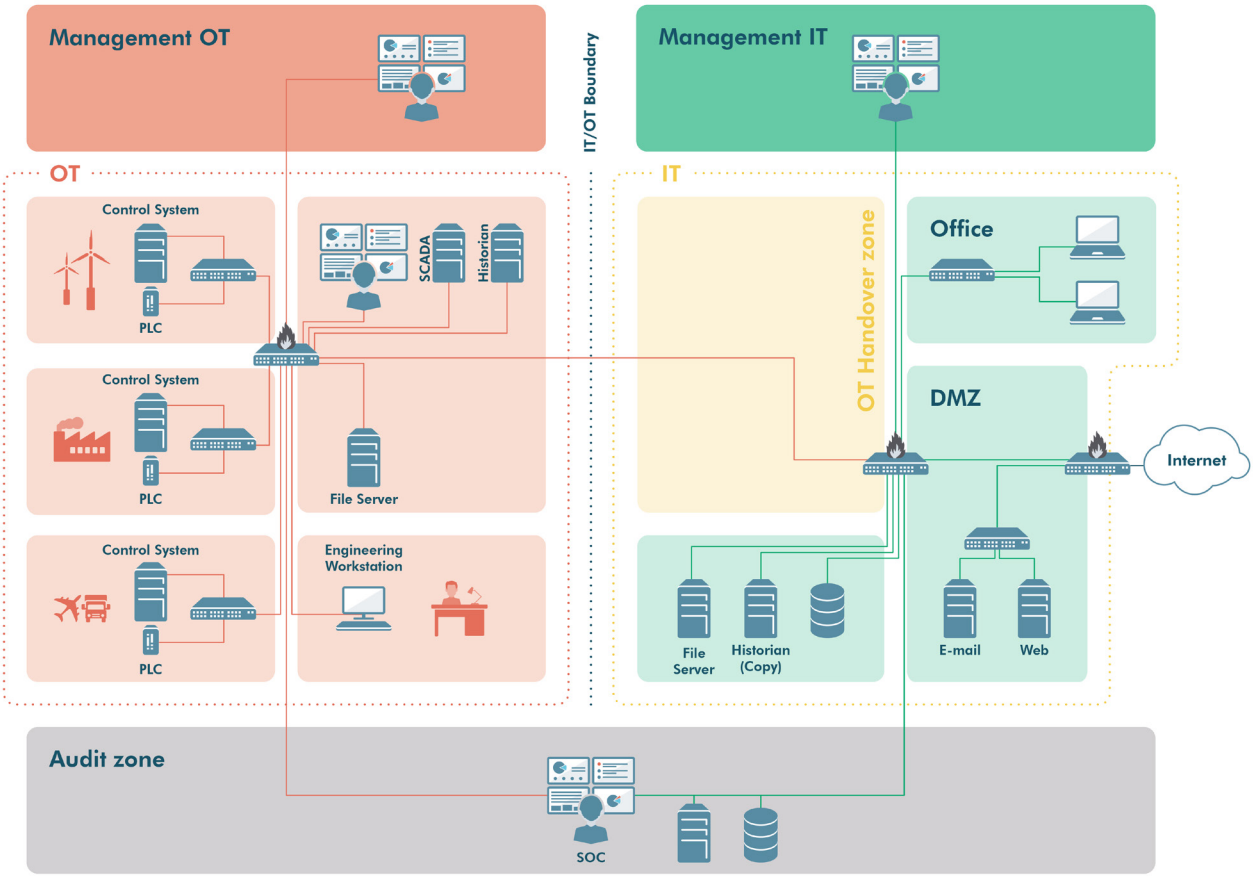
Solution

Network segmentation and zoning

In today's connected world, no system is stronger than its weakest link, and no critical information or system is secure if there is insufficient protection. A cyberattack can result in sensitive and/or critical systems being disrupted, knocked out or leak information. This means that by using zoning, one gathers assets with similar security level and security requirements in separate zones. Segmentation means that you have separate zones for your assets, but most often, you still allow some communication between these zones. In some slightly more extreme cases, isolation or air-gap may be relevant, and then no network-based communication between the zones is allowed. The most critical systems, or the most sensitive information, must be protected with high-assurance solutions in order to obtain a high level of security. A secure way to protect your sensitive information or systems is to start working with network segmentation.

Depending on what zones you want to send information between, and in which direction, you need different solutions. We have created an illustration (Figure 1) which shows an example of different zones in an IT/OT environment. This example is without any high assurance solutions in use.

Figure 1. *Zones in IT/OT environment without high assurance solutions*



Different zones in an IT/OT environment

IT

The IT (Information Technology) zone is where all office related systems reside, such as your personal workstation/laptop, application servers, file servers and intranet. The DMZ (Demilitarised zone), which is part of the IT zone, acts as the handover zone between the organisation's internal systems and the internet. The DMZ hosts systems that are available on the internet, such as Web and e-mail. The OT (Operational Technology) handover zone can also be viewed as an internal DMZ between the IT and OT zones – all traffic going in and out from OT must pass through the OT Handover zone and this is where the IT/OT security controls are located.

The IT zone consists of many different types of systems, devices and people working with these systems. People working in the office must be able to work efficiently, and so the security policies of the IT zone are usually less restrictive than the policies in more security critical zones. It is therefore quite difficult to reach a high enough level of security for a typical IT zone and many attacks against companies and organisations first hit the IT zone.

OT

The OT (Operational Technology) zone hosts systems for controlling and monitoring the physical processes including the processes themselves. These systems usually consist of different types of Industrial Control Systems (ICS) and systems for Supervisory Control and Data Acquisition (SCADA). The OT zone is extremely sensitive for disruptions that would affect systems and processes that are critical for the organisation. Downtime in OT very rapidly transforms to high monetary costs and can also lead to personal injury. Because of the criticality of the OT zone, it must be protected and secured with a high security level. Threat agents are often considered well-financed and competent, which adds to this fact. This is especially the case within critical infrastructure, such as electricity production and distribution.

Audit Zone

The purpose of the audit zone is to monitor (security) events in IT and OT, and to act in case anomalies occur. The Security Operations Centre (SOC) resides withing this zone. From an organisational point of view, the audit zone usually consists of people not related to other parts of the operation. Operating a SOC can be a daunting, resource-intensive task, and therefore some organisations choose to outsource this function to a trusted subcontractor.

Management IT

The Management of IT systems and infrastructure is performed from a separate zone. This zone houses systems and people with administration privileges of IT systems that would cause severe damage if misused or compromised.

Management OT

The Management of OT systems and infrastructure is performed from a separate zone. This zone houses systems and people with administration privileges of OT systems that would cause severe damage if misused or compromised. Management of critical OT systems is considered more sensitive than management of IT systems, i.e. Management OT and Management IT should be placed in different zones.

High assurance solutions in your IT/OT environment

In the illustration on the following page (Figure 2), the different zones have appropriate cybersecurity solutions in the zone borders and explanations of their functions.

Strong segmentation and applying the concept of defence-in-depth are key elements in creating a resilient and secure network architecture. For example, note the number of security controls between a threat agent on the internet and the physical process located in the OT zone. The combination of firewalls, guards and data diodes, each with its strengths and weaknesses form a holistic and comprehensive security architecture. Placing the right security product at the right place is key to success.

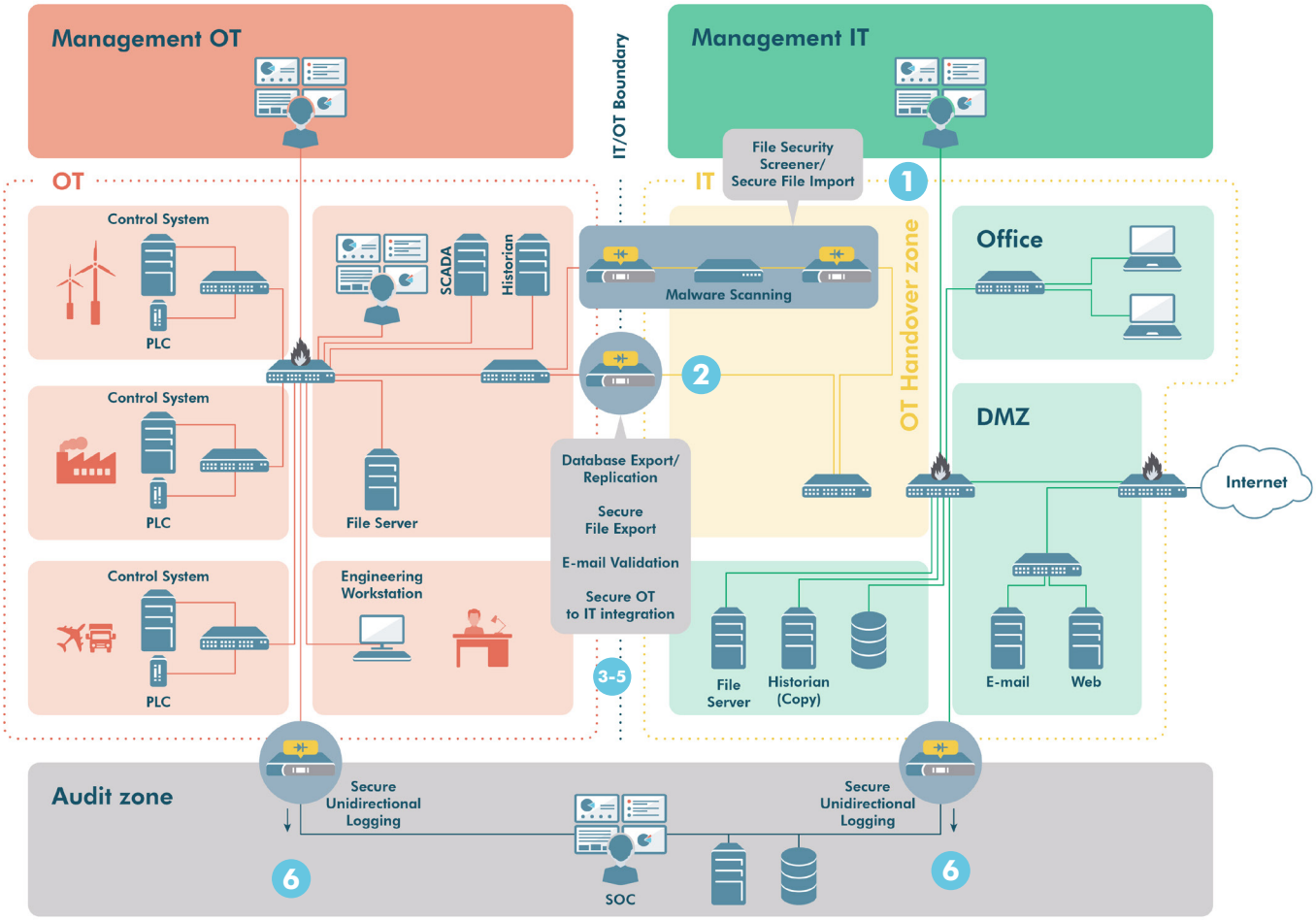


Figure 2. *Zones in IT/OT environment without high assurance solutions*

1. File Security Screener/Secure File Import: Importing files into secure environments poses a great security threat if the files are not properly sanitised before transfer. The File Security Screener is a high assurance Cross Domain Solution with malware security scanning and Content Disarm and Reconstruction (CDR) capabilities.

2. Database Export/Replication: Operators often have the need to export historian data from OT to IT. This can be done using database replication over a data diode. The data diode efficiently protects the integrity and availability of OT and enables the IT side to read measurement data from the process in OT.

3. Secure File Export: Many have the need to export files from an OT environment to an IT environment. Organisations need to keep classified information within the security domain but still have to be able to release information to another system or security domain. The application protects integrity and confidentiality by allowlisting information exchange and provides explicit control over files sent from or to a system.

4. Secure E-mail Validation: A versatile and powerful tool providing policy-based e-mail exchange between network boundaries. Only messages validated by your policy, including attachments, can be sent through an information centric content inspection. The inherent allowlisting works to allow permitted information to be transferred and denies all other information.

5. Secure OT to IT Integration: Digitalisation and efficiency requirements mean that more systems get connected to each other, the Internet or other environments with little knowledge of current vulnerabilities. Secure OT to IT integration using OPC UA is a one-way communication for applications within industrial automation, process control, energy management or other data-intensive systems that makes sure the integration is made secure.

6. Secure Unidirectional Logging: Having centralised auditing is very important in every security architecture. Logging can benefit from having a centralised system for all zones/subsystems, but a centralised system can in itself become a security risk as all systems are connected to the central zone. By using a data diode, you can separate the SOC from OT and thereby eliminate the risk of the SOC interfering with the integrity and availability of the OT systems.