IT/OT integration

Digitalisation drives demand for connecting IT and OT systems. This integration presents security challenges and requires specific solutions.

Challenge

Integrate IT and OT securely

Operational Technology (OT) refers to all the subsystems needed to manage and monitor a physical process, for example at a power station or in a factory. OT usually consists of (among other things) programmable logic controllers (PLCs) and supervisory control and data acquisition (SCADA) systems, but also standard computers and operating systems usually found in an office environment. IT refers to the business and office systems that most organisations use.

Historically, OT systems were often entirely standalone and isolated. However, the need to connect OT to other systems has grown with the digitalisation of society. IT and OT are therefore getting more and more connected, and the same basic technology is often used in IT and OT. The different needs in IT and OT can easily lead to challenging technical conflicts.

Solution

Separate and monitor data flows

Separating IT and OT into separate segments reduces risk of cyber threats migrating from IT to OT. An example would be to get ransomware into your OT environment. To avoid risks as a consequence of mistakes in configuration or function, technology based on physical segmentation is recommended. This means that separate hardware is used for IT and OT.

The most secure way to connect an integrity sensitive OT system to other systems is to use data diodes. All data flows from OT that can be sent over data diodes provides the conditions for a simplified security analysis, quite simply because a data diode is so secure and easy to analyse. Or, more correctly, because it has such high assurance.
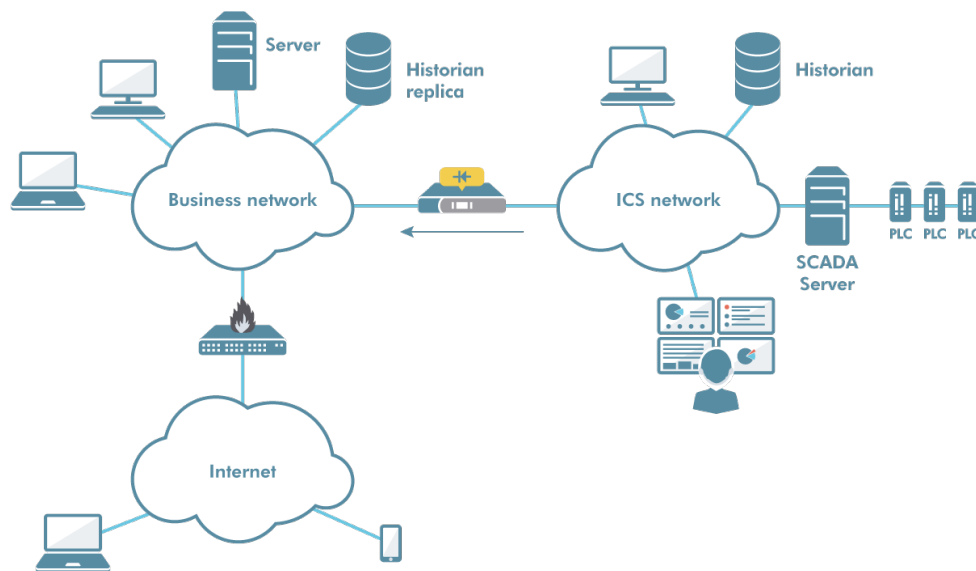
Here are two examples of when using data diodes in an OT environment makes the integration to the IT network more secure:

- **Database mirroring:** One method for exporting data from the OT zone is to mirror the contents of a database from the OT zone. By creating a copy of the data on the IT side, you can allow read access to all IT systems that need to access the database contents.

- **XML export:** Another method is to create an XML file in the OT zone, containing all the data needed outside OT. This file is then sent regularly by FTP/SFTP to a recipient in the IT zone.

Advantages

Optimal balance between function and security

By physically segmenting IT and OT and using data diodes in the zone border, you achieve an optimal balance between function and security. Consequently, you can accelerate the digitalisation process without risking the availability of OT, and you can trust the technology only providing unidirectional traffic flow. Choosing data diodes gives you a future-proof solution that is considerably less likely to need change over time than a solution based on traditional firewalls and intrusion detection systems.