advenica

SOLUTION DESCRIPTION

IT/OT Integration

Digitalisation means that IT and OT systems are connected. This integration presents security challenges and requires special 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 a factory. OT usually consists of programmable logic controllers (PLCs) and supervisory control and data acquisition (SCADA) systems. IT refers to the business and office systems that most organisations use.

Historically, OT systems were often entirely standalone. However, the need to connect OT to other systems has grown with the digitalisation of society. 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 technical conflicts.

Solution

Separate and Monitor Data Flows

Physical separation of IT and OT using zoning

Separating IT and OT into separate segments helps avoid vulnerabilities or disruption in IT affecting OT. To avoid risks as a consequence of mistakes in configuration or function, physical segmentation (zoning) should be used. This means that separate hardware is used for IT and OT.

Use data diodes in the zone border for outbound data flows from OT

The most secure way to connect an integrity sensitive data network to other systems is to use data diodes. All data flows from OT that can be managed with data diodes involve 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.

- 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 contents of the database on the IT side, you can allow read access to all 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.

- Screen mirroring: It is frequently necessary to be able to monitor a process in the OT zone from the IT zone. Creating a screen view in the OT zone and exporting a copy of the screen across the zone border via a data diode permits real-time observation with no risk of the connection being used for attacks on the OT zone. An identical screen view is displayed in the IT zone.

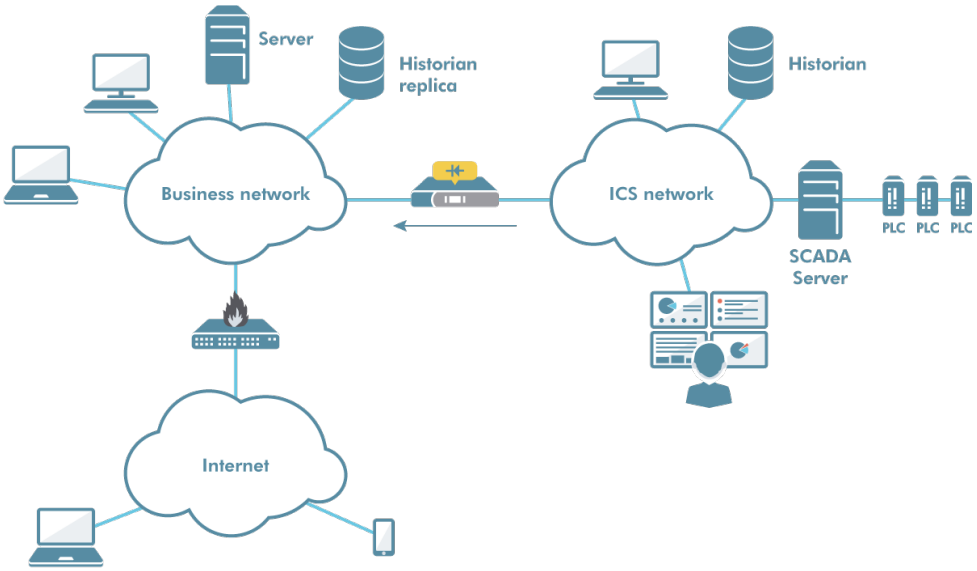
Information whitelisting in the zone border

For data flows for which data diodes are not suitable, you can instead use systems that secure the information flow, such as ZoneGuard. To avoid malicious code intruding and affecting the process, it is important to have strict separation between, and monitoring of, all data flows across the zone border. The most secure method is to have strict control over the information that is permitted to cross the zone border. For example, by not allowing transport protocols to pass the zone border, you entirely avoid many of the risks that you might otherwise face.

Advantages

Optimum Balance Between Function and Security

By physically zoning IT and OT and using data diodes and ZoneGuards in the zone border, you achieve an optimum balance between function and security. Consequently, you can accelerate the digitalisation process without risking the availability of OT, and you also avoid having to spend time and effort on analysing any of the outbound flows from OT. Choosing data diodes and ZoneGuards 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. To read more about our data diodes and ZoneGuard, please visit advenica.com.



advenica

Advenica provides expertise and world-class high assurance cybersecurity solutions for critical data in motion up to Top Secret classification. We enable countries, authorities and companies to raise information security and digitalise responsibly. Founded in 1993, we are EU approved to the highest level of security. Our unique products are designed, developed and manufactured in Sweden.

Read more at advenica.com

ISO 9001 CERTIFIED
ISO 14001 CERTIFIED