
AFRY
ÅF PÖYRY
Cyber
Security OT

Cyber Security OT

The interplay between OT and IT, increased use of new technology, and the ongoing digitization have entailed new threats and risks. This has led to increased awareness, new standards and new regulations. By using expertise, methods, and tools adapted for information security, cybersecurity, continuity planning and disaster recovery planning, we help our customers secure their productions, but also their assets and facilities. The protection of life and health for employees and the environment are important arguments for securing their OT environment.

Operational Technology (OT)

OT is the hardware and software intended to monitor and implement changes in physical processes. This is done through monitoring and control of physical equipment such as valves, pumps, motors, etc. Simply put, OT is the use of computers to monitor and change the physical state of a system.
OT includes i.a. PLC, SCADA, DCS and the network binding all different devices together.

Possibilities

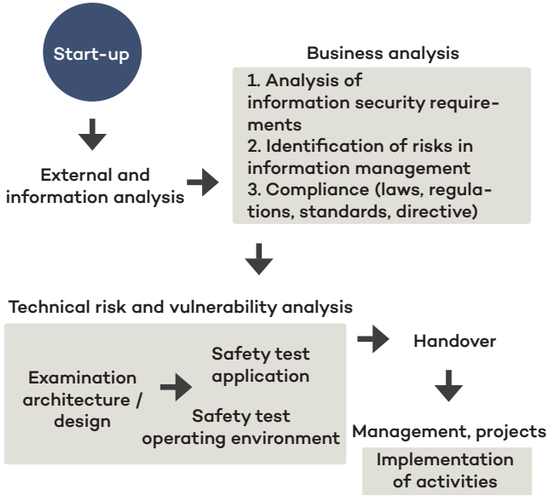
The ongoing digitalization has led to OT and IT getting closer to each other, which has created opportunities to meet old needs in new ways.
For example, processes can be streamlined, costs reduced and resources utilized better.

Threats and risks

The development has brought some new challenges and risks. Attacks such as Stuxnet, BlackEnergy and NotPetya have shown the effect and possibilities of cyber warfare.
This has led to several state's acquired knowledge of both offensive and defensive methods. Another group that has embraced the possibilities of cyber technology are criminals. Criminal groups that previously focused on physical crime have increasingly chosen to focus on cybercrime instead.

Information security analysis

A central method is information security analysis regarding OT. The analysis builds a "map" of the facility's OT and the content, handling and significance of its information.
The analysis leads to implementation of cybersecurity at the right levels and to the proper extent, and to that continuity plans and disaster response plans can be developed.



Methodology

A well-planned protection is based on a number of methods, of which the most important ones are;

Information security: Measures to prevent information is leaked, distorted or destroyed, and ensures that information is available when needed.

Cybersecurity: The protection of OT from theft or damage to its hardware, software, data and protection against disruptions/errors in OT's services.

Continuity planning: Planning of how a plant and its processes should be able to continue to produce with sufficient capacity and quality if it is exposed to disturbances and how to return to a normal state in a controlled manner.

Disaster recovery planning: Methods, tools and routines for restoring OT after a natural or man-made disaster.

Countermeasures

Digitization, interconnected systems and just-in-time production have put the focus on the need to ensure that information always is confidential, accessible, accurate and traceable. Deficiencies in the above can quickly lead to problems and costs. In order to support threat and risk management, several methods have been developed. Within the EU, this has led to the formation of ENISA and the development of the NIS Directive. In Sweden, we have implemented the Security Protection Act 2018: 585, and a national CERT.

Continuous process

Working with information security and cybersecurity is an ongoing process that includes the phases; Identify, Protect, Detect, React and Retrieve.
AFRY's model includes methods, tools and routines, which are based on standards such as ISA / IEC 62443 and ISO 27000, and covers all phases above.

Contact Information

Manager Industrial Digitalization OT
Martin Hagelthorn
+46 (0) 10 505 4087
martin.hagelthorn@afry.com

Cyber Security Architect OT
Jacob Hinsch
+46 (0) 72 003 0564
+45 222 191 00
jacob.hinsch@afry.com

Cyber Security Architect OT
Hans Arve Arvesen
+46 (0) 10 505 2744
hansarve.arvesen@afry.com

Manager Industrial Digitalization
Nico Dima
+46 (0) 10 505 5027
nico.dima@afry.com

Denmark
Kasper Nilsen
+45 40 26 2694
nico.dima@afry.com

Sales
Per André
+46 (0) 10 505 4538
per.andre@afry.com

Robert Fahlborg
+46 (0) 10 505 6642
robert.fahlborg@afry.com

Björn Hellström
+46 (0) 10 505 2489
bjorn.hellstrom@afry.com

VP and Head of Business Area Advanced Automation
Michael Mjörnestål
+46 (0) 10 505 6358
michael.mjornestal@afry.com

AFRY
ÅF PÖYRY