advenica

5 steps for a secure IT/OT integration

We have listed 5 steps for how you can securely integrate IT/OT! The method is based upon the standard IEC 62443 – a must for those who work with security within OT.

1. Identify the system

The main purpose of this step is to define the project scope and to decide what to segment. The SCADA system often contains information that you want to export to the office environment. You may also need to maintain the OT/SCADA environment and thus import data from the office environment.

2. Initial risk analysis

The next step is to make an initial, simple risk analysis and identify the present worst-case scenario before having introduced any risk reduction measures. Based on this, you can later make a first grouping of systems and flows. You need to define your most critial system assets, consequences and the probability of those consequenses and based on that, a worst-case risk that the various parts of the system are exposed to without security functions or segmentation can be calculated. By placing the scenarios on a scale of consequence level, it becomes clear which scenario is considered the most serious.

3. Zoning och dataflows

Base the grouping on the risk analysis, but also involve best practices and reference architectures. When the systems are placed in zones, they are divided into e.g. Office, DMZ, SCADA and Facilities. When it comes to segmenting data flows, it can be difficult and complex to figure out which they are. You can do a traffic analysis to find out what protocols you have and what is going on in the network. One way to do this is by recording traffic from your network and then viewing the traffic with analysis tools. After doing a traffic analysis, you can see what kind of data that is flowing between the zones.

4. Detailed risk analysis

According to IEC 62443, a detailed risk analysis should be performed if the initial risk exceeds the acceptable risk. In the detailed risk analysis, one risk analysis is performed per zone and flow. The same risk matrix and method as in the initial risk analysis should be used. When the reduced risk is smaller than the acceptable risk, you have reached the goal of your risk-reducing measures.

5. Design

When you have completed the detailed risk analysis, it is time to focus on design. The design will be the result of your analyses – what the final segmentation solution will look like. One solution to ensure that the data flows in a one-way direction out of the zones is to use data diodes. You can create a one-way export channel of measurement data using a data diode. IEC 62443 defines 5 security levels that help to derive security-related requirements and define the strength of the segmentation solution.

advenica

ISO 9001
CERTIFIED
ISO 14001
CERTIFIED