Secura
A BUREAU VERITAS COMPANY

OT Site Assessment

As industrial control systems become more connected, they also become more exposed to cyber threats. The consequences of a cyberattack could negatively affect the organization's efficiency, continuity, and even safety. Addressing these risks is essential for organizations looking to protect their Industrial Control Systems (ICS).

What are common concerns in the ICS industry?

Cyberattacks on ICS and SCADA systems can impact the **safety**, **availability**, and **reliability** of systems, operations, and value chains leading to catastrophic consequences. Organizations that are potentially impacted by these consequences are located in various industries, including but not limited to electric power, water, nuclear, manufacturing, infrastructure, transport (railways, ports, and airports), and oil & gas (upstream, midstream, downstream).

Organizations within these industries have a variety of concerns such as cyberattacks that could cause **damage to reputation**, **shareholder confidence**, **environment**, or cause **system outage**, **loss of production**, **injury**, or even **loss of life**. Organizations therefore must assess if they have the right mitigations in place to sustain ICS security. While IT and OT have been increasingly convergent over the years, a gap in understanding and solid practice between OT and IT security tends to remain. This critical skills gap contributes to security vulnerabilities, which are often overseen but must be identified and addressed appropriately.

At the same time government regulations grow as cyberattacks increase in frequency and severity leading to significant challenges in compliance. There are many standards, but they vary greatly and the ones that apply are not being made by operator choice, but rather by regulation based on industry alignment. Organizations are often unclear on how to apply these standards within their environment. Secura helps organizations by providing guidance and enabling them to regain control over their OT security. Secura provides organizations with the capabilities to regain control over their OT Security.

How can Secura help your organization?

Secura has developed a proven OT site assessment methodology that follows internationally recognized standards and best practices such as **IEC 62443**, **NIST SP 800-82**, and **ALARP** which are specifically tailored to **Industrial Automation Control Systems (IACS)**. The OT Site Assessment is specifically designed to identify technical site-level risks as opposed to organizational-level risks. It is a bottom-up approach that includes site visits, system architecture reviews, and interviews with subject matter experts. Optionally the assessment can be expanded with high-level penetration testing to verify the level of protection between IT-OT or passive packet capture and analysis. The OT site assessment service includes the following IEC 62443 aspects and addresses the following subject areas within each aspect:

IEC 62443	OT Site Assessment Areas	
FR 1 **Identification and authentication control**	Assessing the extent of **insider risks** focusing on the impact that can be caused per group of insiders based on existing mitigating controls.	Assessing potential **cyber-physical attack risks** by analysing process flow diagram outputs, conducting SME interviews and analysing industry incident reports deriving to real attack scenarios.
FR 2 **Use control**	Investigating **external exposure** in the form of undesirable externally accessible domains, IPs and modem connectivity as well as physical security vulnerabilities of the entire site which could impact the availability and safety of the site.	
FR 3 **System integrity**	Assessing **OT Network Traffic analysis** to discover various kinds of connectivity present on-site, exposure outside of designated areas and physical perimeters and any security issues that can be identified passively.	
	Assessing the **inherent cyber resilience** of your organization both on an architectural and configuration level.	
FR 4 **Data confidentiality**	Assessing **data exfiltration risks** such as obtaining intellectual property and corporate secrets up to obtaining technical information to prepare sabotage.	
FR 5 **Restricted data flow**	**Collecting Network Traffic** passively at agreed-upon locations utilizing passive network taps or monitor ports. No active scanning, man-in-the-middle or other measures which might interfere with traffic will be used.	
FR 6 **Timely response to events**	Assessing **OT network and systems security** aiming to see if malicious entities can get into your OT network and see what they can potentially compromise (e.g. by checking firewall configuration, lateral movement and checking for insecure protocols).	
FR 7 **Resource availability**		
	Conducting a discrepancy analysis between asset inventory, architecture maps and perimeter to see whether **ICS Visibility and Control** is addressed coherently.	

What are the deliverables?

A detailed OT site assessment report will be delivered with **all identified risks**, each with an **explanation** and **recommendation**. All findings are given a qualitative **risk rating**. Secura follows a standard risk rating system which can be adjusted based on your organization. Not only are the risks to the ICS identified, but areas to sustain are also included in the report indicating the **security strengths** of the facility in scope. (The graphical overview as presented in Figure 1 is showcasing an example of how all the identified risks are reported and mapped to IEC 62443 foundational requirements)

Cyber-physical attack scenarios are outlined by giving a detailed description of how an attacker could potentially target the specific site in scope. Cyber-physical attack scenarios could encompass all functional requirements of IEC 62443.

What are the results?

The results of the OT Site Assessment presented by Secura will provide you with the following insights:

- How effective the implemented OT security controls are;
- How these risks are mapped to relevant parts of the IEC 62443 requirements;
- Were improvements might be required, including our recommendations.

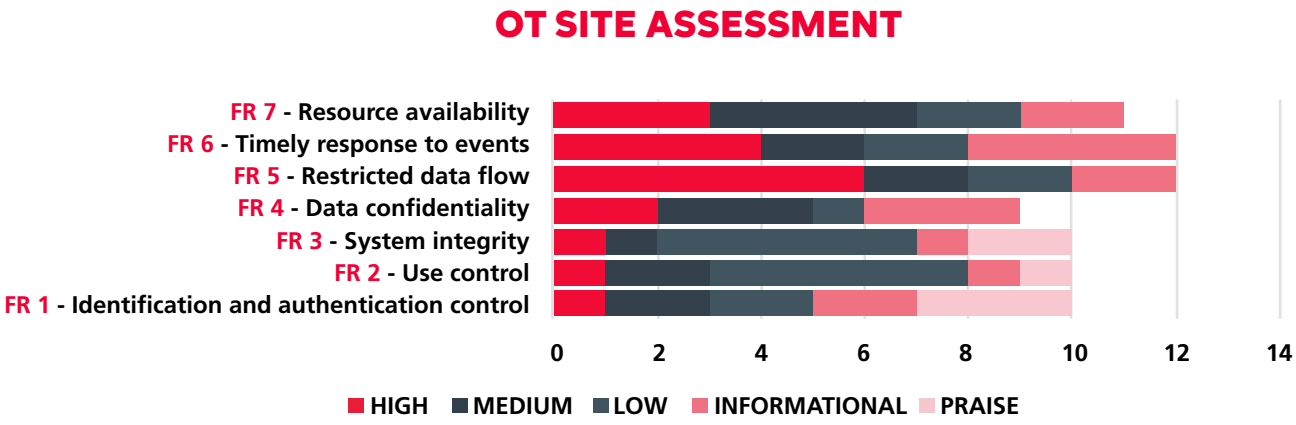

Figure 1. Example of a graphic overview within the OT Site Assessment Report

Why Secura?

Secura believes it is important that OT security is addressed to the highest level achievable, considering the impact a cybersecurity attack may have on health, safety and the environment. We support organizations across various industries in their journey to improve their OT security. Secura is experienced in delivering security and visibility for some of the world's most complex OT networks including Europe's largest manufacturing facility and other various key players in critical infrastructure. We guide organizations in **understanding risks, gaps and vulnerabilities in industrial control systems** by using a layered approach considering the **NIS and NIST compliance frameworks** for critical infrastructure. The value of Secura comes forth in **approaching OT security from well-known and internationally recognized ICS standards** required by the regulations of various countries or distinct areas in the world.

Not only does Secura understand what is required by world's most known and accepted ICS standards, but our **team of experts also possesses the necessary engineering understanding to identify and interpret the impact of vulnerabilities** in distinct OT environments consisting out of Stand-Alone, Distributed and/or Supervisory Control and Data Acquisition systems. Secura **identifies threats and risks** to OT systems by continuously investing in the training and education of its dedicated consultants.

Secura requires that its consultants have the right **cybersecurity and engineering knowledge** including but not limited to control loops, plant organization (as per ISA-88), architecture, data flows, connectivity and commonly used diagrams such as process flow diagrams and piping and instrumentation diagrams to identify specific cyber risks related to PLCs, PACs, RTUs and Safety Instrumented Systems (SIS). The cybersecurity and engineering understanding of our consultants bring them at the forefront of OT security in the world translating to understanding the concerns of our clients and providing state-of-the-art solutions based on well-recognized standards for each distinct area of the world.

Secura
A BUREAU VERITAS COMPANY

Interested?

Contact us today:

Follow us:

+31 88 888 3100
info@secura.com
secura.com

BUREAU VERITAS
1828

Shaping a World of Trust