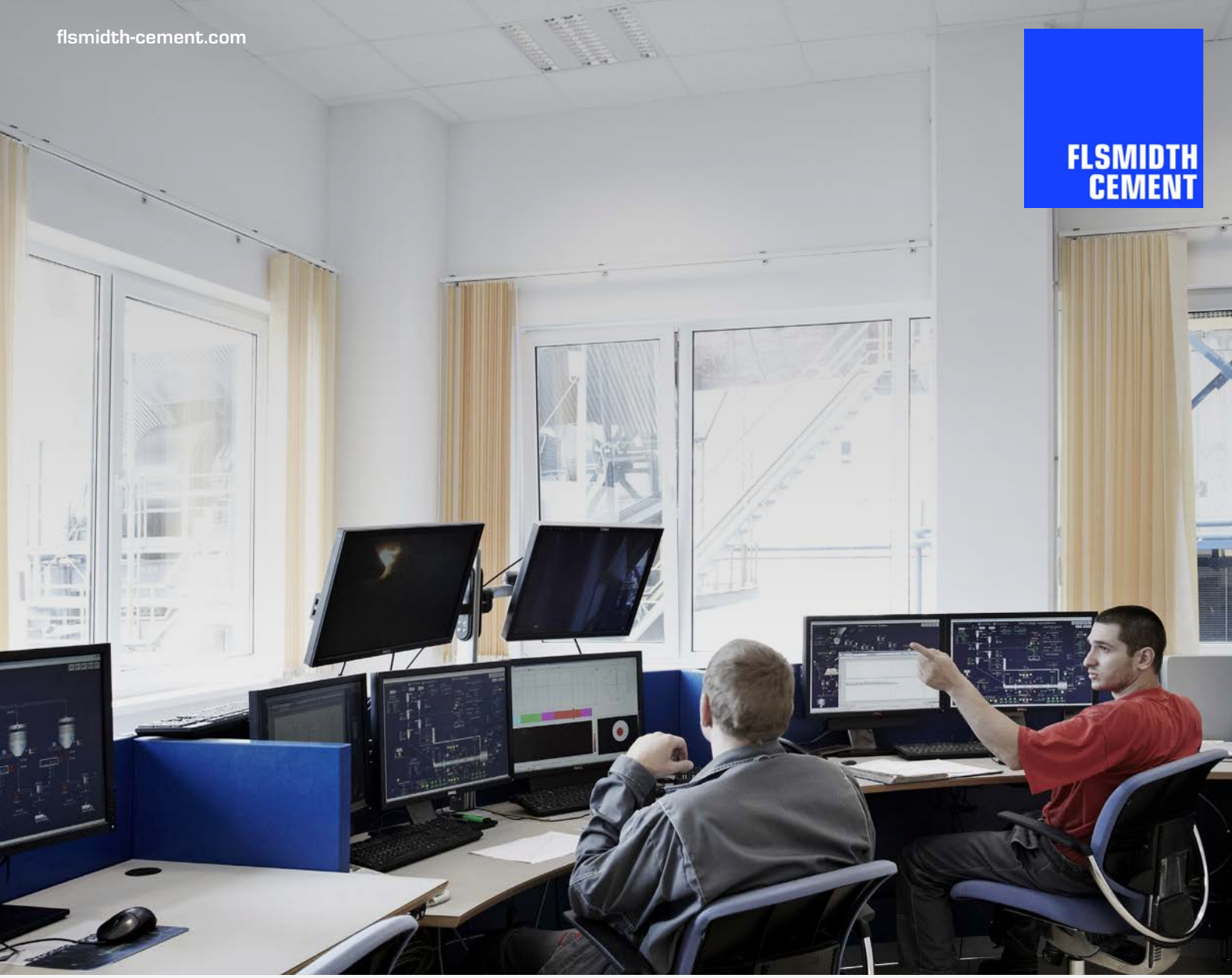


CYBERSECURITY ASSESSMENTS THAT UNDERPIN RELIABLE CYBER DEFENCE

Integrating our knowledge of IT and OT systems, our cyber-security assessments provide comprehensive insight into vulnerabilities and prevent critical damage to plant control and automation systems.

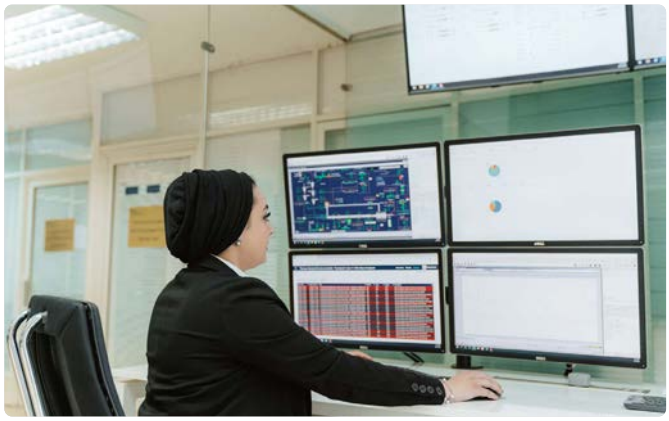
KEY BENEFITS

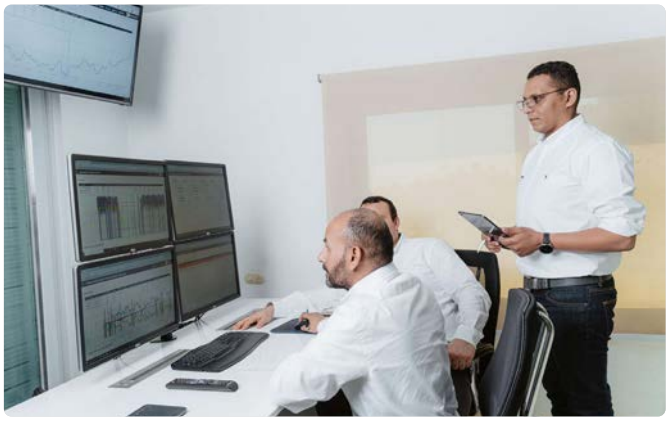
- IT-OT integration for complete picture of potential vulnerabilities
- Integrate with PlantLine service agreement
- Access expert 24/7 cybersecurity support.

WHY DO I NEED A CYBERSECURITY ASSESSMENT?

Industry 4.0 is connecting industrial process as never before and transforming the way industries operate. But greater connectivity brings with it greater exposure to critical cybersecurity risks. The frequency cyberattacks on industrial control systems has increased at an alarming rate in recent years.

The stats speak for themselves. According to the industrial cybersecurity experts at Dragos Security, there was an 87% increase in ransomware attacks on industrial organisations in 2022 and a 35% increase in ransomware groups targeting industrial control and operational technologies (OT) systems.[1] Figures from Kaspersky ICS CERT indicate that 2022 was the year with the highest percentage of OT computers protected from malware.[2]





A risk you ignore at your peril

The cost of an industrial cyberattack will vary according to its severity and the size of the company, but the impact can be significant. Malware infection of a plant control or other automation system can quickly bring production to a halt. In worst case scenarios, it may even result in damage to critical OT systems, putting personnel at risk of harm and causing negative environmental impacts.

Industrial automation systems are also typically older, unpatched, and thus more vulnerable to cyberattack. All this means it might be time to consider a comprehensive cybersecurity assessment of your plant control and automation systems. And who better to undertake that assessment than the experts who supplied both your equipment and automation systems?

Integrating IT and OT for a truly comprehensive approach

There are many companies out there offering cybersecurity assessments. But there's only one that knows you, your OT systems, and your operating processes from the inside out. That's us. Because we understand the relationship between IT and OT, we bring greater depth of insight to the cybersecurity assessment process. We not only assess and report system risks; we also recommend prioritised investment to strengthen your cybersecurity systems to ensure your plant is protected from cyberattack.

[1] Dragos ISC/OT Cybersecurity Year in Review (February 2023).

[2] Kaspersky ICS CERT 'Industrial sector attacks on the rise: an annual overview by Kaspersky' (March 2023).

How do I know if I need a cybersecurity assessment?

If you answer 'no' to any of the following questions, we recommend you undertake a cybersecurity assessment as soon as possible:

- Do you have an up-to-date inventory of all devices on your automation network?
- Are critical devices patched and free of known vulnerabilities?
- Are you sure that there is no unauthorised software installed on OT servers or clients?
- Are you sure that there are no unauthorised internet connections or devices with multiple network connections?
- Is your firewall up to date and correctly configured?
- Are USB ports blocked or protected from malware execution?
- Are administrative accounts secured and not used for other purposes?
- Are backups taken regularly and stored securely; are you sure that an attacker could not access them; are they tested?
- Is antivirus software installed and kept up to date on all devices?
- Do you have a prober insight and understanding of which and how devices are communicating on the network?

WHAT DOES A CYBERSECURITY ASSESSMENT FROM FLSMIDTH INVOLVE?

Our cybersecurity assessments are tailored to match your needs and the equipment you have onsite. A typical assessment comprises:

- A review of existing FLSmidth drawings and documentation.
- Remote information gathering via Go2FLS remote access (if available).
- Information from FLSmidth McAfee antivirus server (if used).
- Online meeting with customer to clarify outstanding questions.
- Onsite visit to clarify and complete the information-gathering process, including observations, interviews, and passive data-collection tools:
  - Verification of existing documentation and asset list.
  - Collection of asset inventory in plant automation network(s).
  - Review of lifecycle support status and firmware/patch status, considering any known vulnerabilities.
  - Verification of systems configuration in scope (e.g. servers, clients, PLCs, switches, and firewall)
  - Review and verification of the existing network drawings.
  - Review of IT-OT communication.
  - Review of backup and restore procedures.
  - Review and verification of systems configuration backups.
- Presentation of results:
  - Report on current status with recommendations based on cybersecurity standards, best practices, and the information gathered.
  - Executive summary of the results and recommendations.
  - Asset inventory of programmable devices, with lifecycle status and recommendations, including prioritised list of recommendations for upgrades or replacements.
  - Updated network and configuration drawings
  - Online meeting to present the results.

Additionally – when requested – we can work with you to secure your systems based on the findings of the assessment. This may include:

- A prioritised investment plan for required upgrades, replacement of obsolete equipment, or other mitigations.
- Making configuration changes or other mitigations, either as part of planned maintenance visits, remotely as part of a PlantLine service agreement, or in a further dedicated site visit.
- Supporting you to implement mitigations yourself with detailed instructions.
- OT network security monitoring integration with your existing security operations centre (SOC) or FLSmidth's security partner.

A WHOLISTIC CYBERSECURITY APPROACH

Go2FLS remote access

Our remote services are a well-established part of our PLA offering. Enabled by our Go2FLS technology, we can remotely access your plant's control network for internal plant support and maintenance, tapping in to real-time process mimics, trends, diagnostic faceplates, and all alarms/events on the plant's control system. It means we can be part of troubleshooting efforts, engineering, software maintenance and process optimisation, wherever you are located in the world. Go2FLS also allows us to undertake initial information gathering for cybersecurity assessments remotely, allowing any time we spend at your plant to be optimised to those tasks that most need us there.

Managed whitelisting service

Antivirus software can protect your systems against known malware, but not against unknown (called zero-day) threats. To add more safety than the traditional antivirus can deliver, we therefore offer managed whitelisting software on a subscription basis, including licenses, update tests, monitoring, support, and reporting. This service allows only existing software to run on your PCs and is therefore an excellent option to improve cybersecurity in the relatively static world of industrial automation software.

System hardening

System hardening aims to eliminate means of attack by turning off non-essential services. Our system hardening service covers FLSmidth-supplied PCs, PLCs, firewalls, and network equipment. It involves configuration checks, back-ups, Windows OS/firmware patching, and hardening of equipment, and can be offered as a remote or onsite service, or as a combination of the two, to meet the requirements of the individual customer or site(s). Checks are performed using a standard checklist, prepared based on industry best practices and recommendations for FLSmidth products.

C 01-24 800-36-ENG