
SECURE
Cybersecurity helps prevent industrial businesses from losing operational control due to internal or external cyber threats.
se.com/industrial-automation-solutions
Life Is On
Schneider Electric

Table of contents

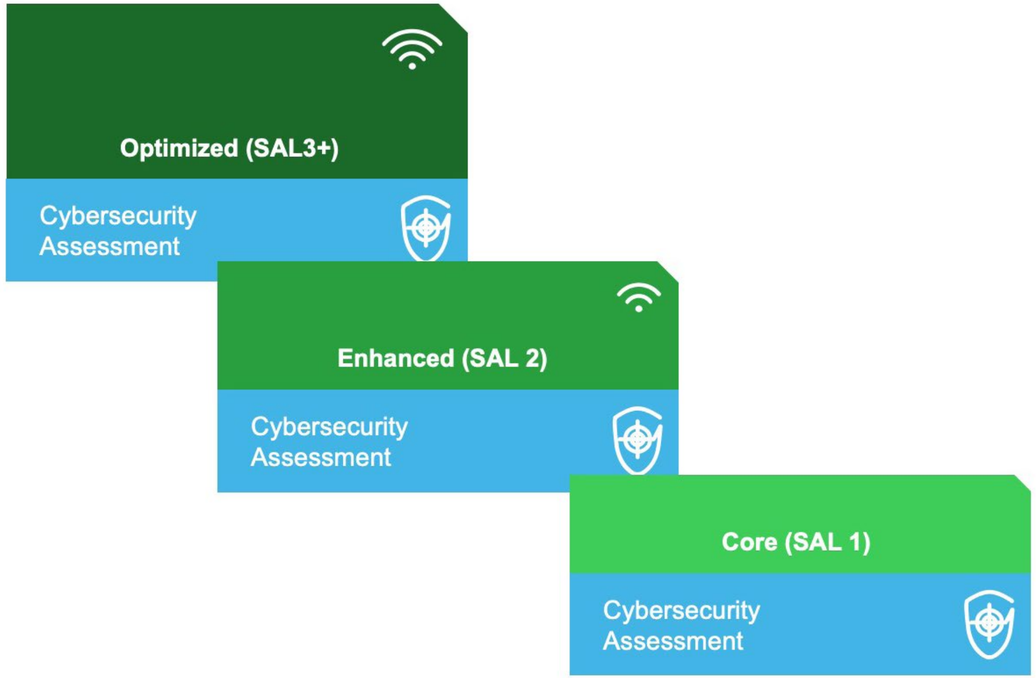
- Do you need gap analysis and guidance to comply with regulations or international standards?
- Do you need an assessment approach that is scalable and can adapt to different maturity levels?
- Do you need an expert analysis to identify and prioritize gaps and recommended steps to close them?
- Do you want an expert consultation to help you develop a cybersecurity roadmap?

Cybersecurity Assessment Service (CAS) extended

is your answer to help you identify cybersecurity gaps and then define a tangible roadmap to close them.

Cybersecurity Assessment Service (CAS) extended

Solution



The CAS evaluates current your present status versus cybersecurity industry standards; the output is a detailed report completed by an OT cybersecurity expert that helps to identify your gaps and defines a tangible plan to close them.

Why it matters?

- The assessment is completed by an experienced expert that has both OT/IT and cybersecurity knowledge
- The assessment is vendor-agnostic and can be completed standalone or part of a larger project
- The recommendation roadmap helps you to maximize your cybersecurity budget
- Assessment is aligned to the globally accepted OT cybersecurity standard (IEC 62443)

Learn more about how this cybersecurity solution can work for you.

- Do you require holistic visibility and actionable cybersecurity data insights in your architecture?
- Do you expect predictable timelines and cost to integrate cybersecurity in your projects?
- Do you need routine, standardized, uniform approach to implement cybersecurity controls?

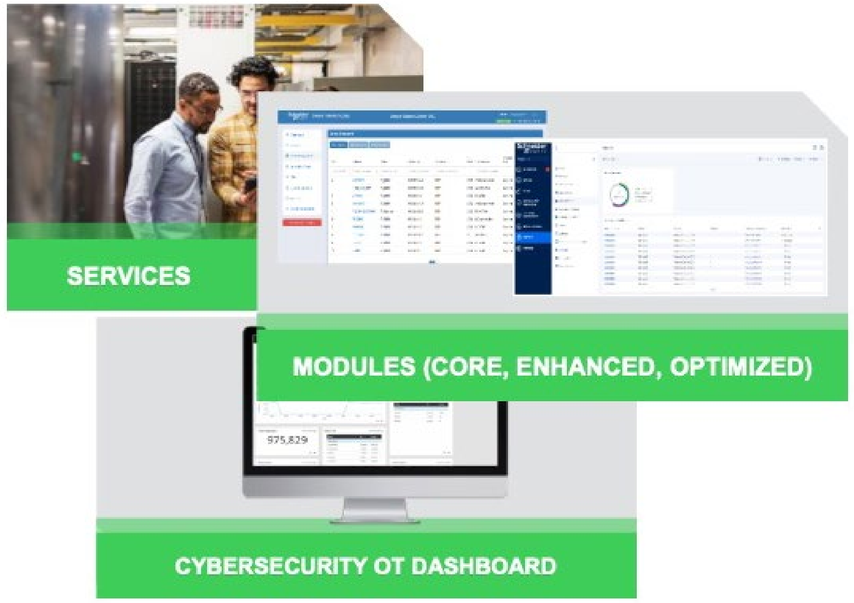
Cybersecurity Application Platform (CAP) packages

may be the answer you need to help you improve and align to IEC 62443 requirements by providing a roadmap and solution for cybersecurity.

Cybersecurity Application Platform (CAP) packages

Solution

- Cybersecurity OT dashboard
- Packages (Core, Enhanced, Optimized)
- Expert Services by subscription



This integrated cybersecurity solution provides operations teams with visibility of key cybersecurity data so they can take action to manage/ maintain cybersecurity control points. Modules and service levels can be customized to meet specific needs.

Why it matters?

System security to protect data and assets

- Help ensure business continuity
- Reduce the risk of cybersecurity attacks
- Help secure plant operations

Built in security features

- CAP packages structured to align to IEC 62443 requirements, providing a roadmap and solution to help customers improve their security year over year

One platform used to monitor and maintain cybersecurity controls

Learn more about how this cybersecurity solution can work for you.

- Do you need to enhance your protection level by adding network security and perimeter security layers?
- Do you require predictable timelines and cost to integrate cybersecurity in your projects?
- Do you need a holistic visibility and actionable cybersecurity data insights in your architecture?
- Do you need active processes to monitor the operating environment to detect and communicate threats?
- Do you want capabilities and systems which support rapid response to cyber incidents to contain and mitigate attacks?

Cybersecurity brownfield plant automation architecture

Cyber-secure brownfield plant automation architecture is the solution you have been looking for to help you be ready for the digital revolution.

Cyber-secure brownfield plant automation architecture

Solution architecture

An enhanced Ethernet network and perimeter security solution which provides better security protection. This solution from our technology partner integrated into our Harmony Edge Box provides these features with minimum impact to existing architectures.

Why it matters?

System security to help protect data and assets

- Help ensure business continuity
- Reduced risk of security attack
- More secure plant operations

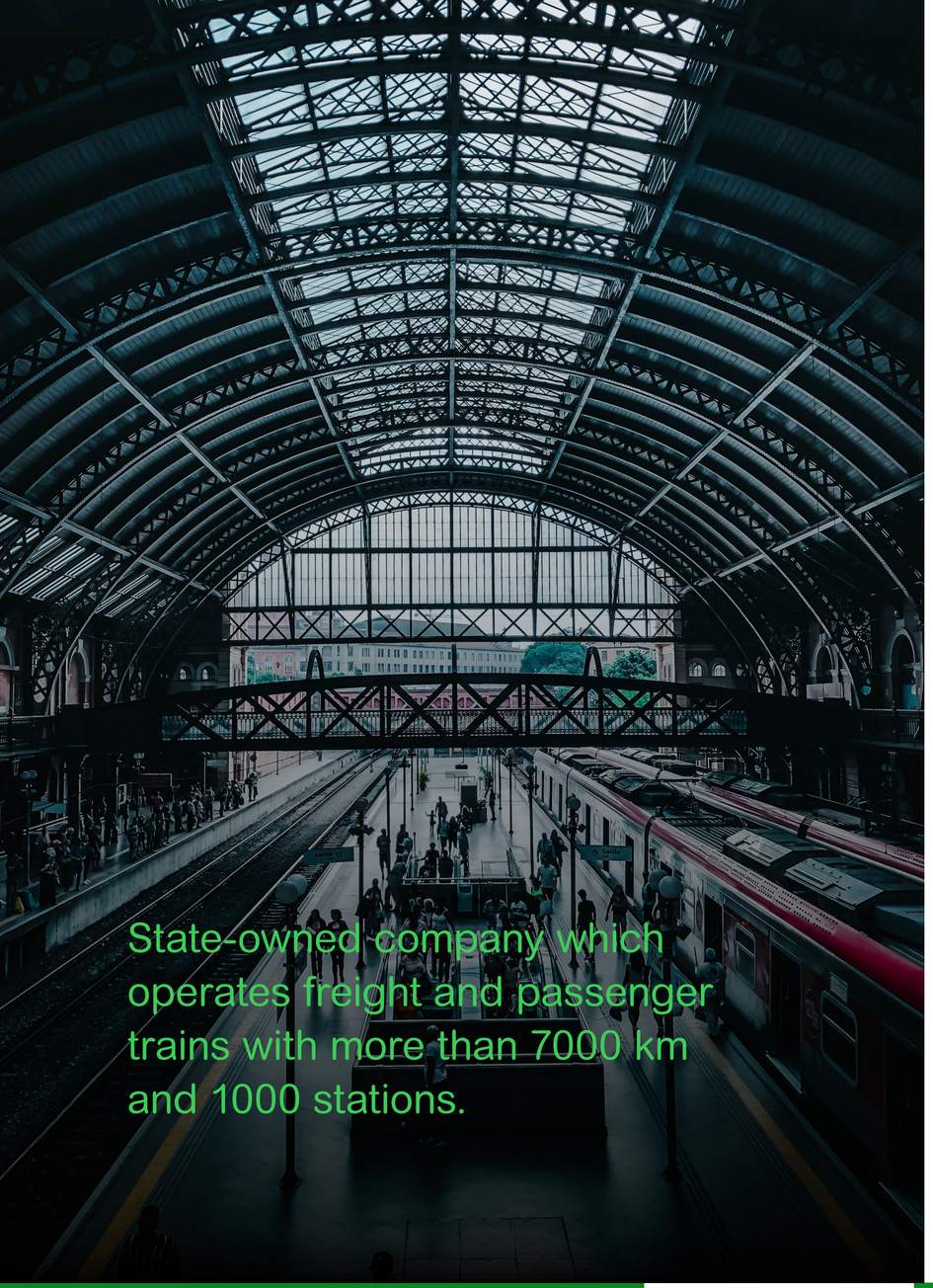
Significant improvements in plant security protection with minimum impact to existing network architectures and automation devices

Compatible with a holistic approach to a location's security plan

Helps meet security standards and comply with regulations

- Help prevent cyber issues from affecting factory/brand image
- Valued by cybersecurity conscious consumers

Learn more about how this cybersecurity solution works for a **state-owned rail company.**



Brownfield Plant

Cyber-attacks on Industrial Control Systems are becoming more prevalent. These systems are generally easy targets for attackers due to their extended life expectancy and their dependence on legacy technologies. Many Systems did not consider cybersecurity during their conceptual definition and as a result are vulnerable to even the most basic attacks.

The solution focuses on brownfield plants, where the migration of installed base PLCs or network infrastructure is not possible in the short term. The solution has minimum impact at the level of existing network infrastructure and zero re-configuration of existing automation assets.

Schneider Electric has selected IEC 62443 as its core cybersecurity standard and provides transportation facility operators with end-to-end cybersecurity surrounding their digital solutions as part of their cybersecurity strategy.

Customer benefits

- Fast implementation
- Quick return on investment
- Scalable solution
- Solution open to OT and IT
- Able to connect disparate automation systems and collate usage information for analysis

Learn more

- Do you need a secure remote access to timely response in case of an unexpected event?
- Do you need to reduce downtime and travel costs for maintenance tasks?
- Do you need to manage and remotely diagnose or maintain assets?
- Do you want to securely connect to advanced asset performance and analytics?

A secure remote maintenance operations solution

is a cybersecure remote access tool to diagnose and troubleshoot equipment from almost any location as if you were on site.

Secure remote maintenance operations

Solution architecture

Reduce downtime and travel costs with a Secure Connect solution. It uses Schneider Electric software to access HMIs, PLCs, or Drives, giving you a cybersecure tool to diagnose and troubleshoot equipment as if you were on site.

Why it matters?

- Component of secure IT infrastructure that provides confidence to allow asset connectivity
- Complete Cybersecure automation system is easy to configure based on IIoT Box and M580
- Easy step to start your digitization journey – even for existing installations.
- Help to comply with regulations
  - Enable new engineering and maintenance models
- Help maintenance teams make the right decisions remotely.
- Possible to access remote expertise without IT department assistance.
- Travel cost reduction and rapid access to remote, on-line support.

Learn more about how this cybersecurity solution works for **Pet Food Production.**

Pet food production machinery OEM Secure remote maintenance operations

Customer challenge

Gain access to all the insights required for machine supervision. This required advanced local HMI capabilities with high-quality graphics and traceability combined with direct remote access to the machine, including its controller for remote diagnostics and troubleshooting.

The solution

EcoStruxure Secure Connect Advisor for secure remote access and EcoStruxure Machine SCADA Expert for complete local supervision, including high-quality graphs and traceability features.

Results

- Remote access to the M340 controller at the customer facility
- Ability to perform configuration, commissioning, calibration, online diagnostics analysis etc., remotely from the OEM's computers (e.g. back at their offices)
- Reduced downtime and associated costs
- High-quality graphs and insights available to support process optimization and traceability requirements for the CPG segment

Learn more

- Do you need a blueprint for the essential security and connectivity foundation required to deploy and implement industry 4.0 and IIoT concepts and models?
- Do you want to digitize industrial and production environments to achieve significantly improved business operation outcomes?
- Do you require documentation and secure reference architecture as part of your common defense in depth strategy?
- Do you need to authenticate all user and machines before authorizing any action at control level?

Secure Architecture with M580 End-to-End Cybersecurity

is the answer you have been looking for to secure and defend against cyber threats to protect your plant network.

Secure Architecture with M580 End-to-End Cybersecurity

Solution architecture

Protecting business making plant networks more secure with defence against cyber threats.

Why it matters?

Architecture compliance with 62443-3-3

- Built in security capabilities
  - OPC UA advanced security features e.g with certificate authority integration
  - Secure Engineering link Modbus over https
  - Secure firmware download
  - Firmware integrity
  - In-rack IPsec-VPN capabilities for EIP/Modbus
- Designed for Critical Infrastructure and Essential Services providers
- Help maintenance teams make the right decisions remotely
- System security to protect data and assets
- Ensured business continuity
- Secure plant operation

Learn more about how this cybersecurity solution works for **Industry #1 Beverage Company in UK**

Industry #1 Beverage Company, UK

Customer challenge

- Remote access cybersecurity solution
- 141 global manufacturing sites
- Remote desktop solution offering full IT/OT separation & military grade hardware
- Multi-factor authentication
- Configuration & user management.
- Threat analysis & patch management

The solution

- Solution customized to meet customer’s global operation demands
- Customer relationship management by Schneider UK team
- Local installation and site support offer

Results

- Regional security expertise supported by global organization
- Fully compliant with ISA/IEC62443
- Ongoing comprehensive service offer
- OT provider with IT expertise
- traceability requirements for the CPG segment

Life Is On | Schneider Electric

To learn more about how cybersecurity helps prevent industrial businesses from losing operational control due to internal or external cyber threats visit

se.com/industrial-automation-solutions

Schneider Electric
35 rue Joseph Monier
92500 Rueil-Malmaison, France
Tel : +33 (0)1 41 29 70 00

998-22931059