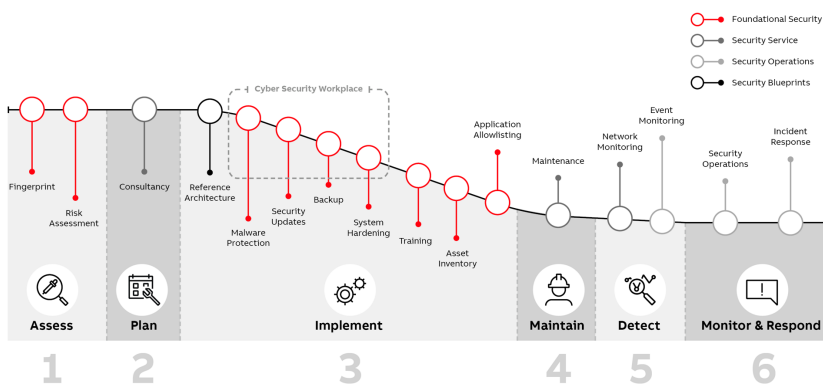# The building blocks for cyber security

—
The industrial cyber
security journey

Operational Technology (OT) cyber security is an increasing priority for operating companies and regulators alike and the industry statistics show why this is:

- 350,000 new malicious programs (malware) are detected each day! Adding to the total amount of over 1.2B known ones
- 81% of CISOs in the energy sector has seen a clear rise in attacks over the past 12 months

Understanding and managing the risks associated with a cyber-attack and then protecting against these or mitigating the consequences can seem a daunting prospect especially when this needs to be done in conjunction with the day job of keep a plant up and running. The old adage of it's a journey not a destination is very true when it comes to OT cyber security.

ABB can support companies with this journey and can do so in small "bite sized" steps to help companies take the next step.

Cyber security assessment - Benchmark
Cyber security benchmark collects system data to identify areas of your control system that are most vulnerable to security breaches. It uses non-invasive data gathering collection tool and provides a colour coded report highlighting areas for improvement. This report provides you with an instant view of the health of your system's security.

Benefits
- Provides basic understanding of where to improve your cyber security
- Accelerates problem solving by providing visualization of your control system security status
- Improves cyber awareness
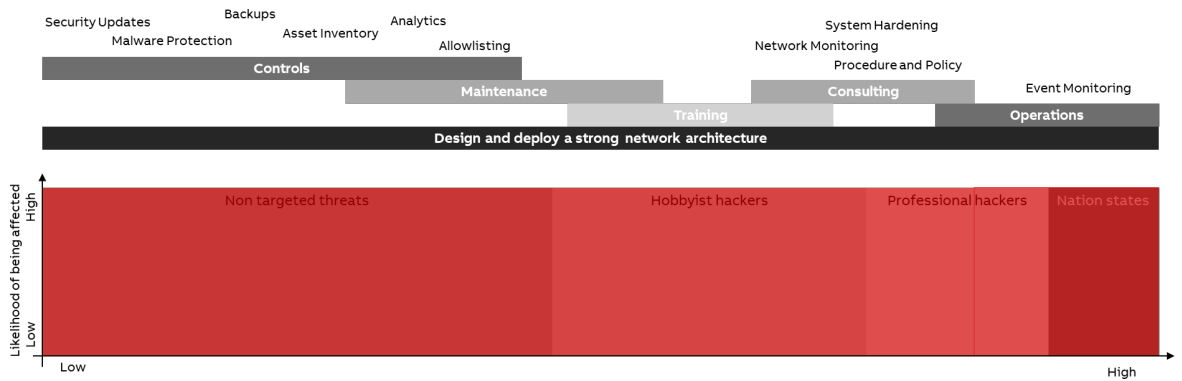- Enables compliance with regulatory standards
- Better IT/OT Collaboration

Cyber security assessment - Fingerprint
ABB cyber security fingerprint identifies strengths and weaknesses for defending against a cyber attack within a plant's control systems. This software-based analysis tool gathers and analyzes data from critical system configurations and compares them against industry standards. The resulting report provides detailed recommendations to reduce cyber security vulnerabilities while helping to develop a focused and sustainable security strategy for control systems.

Benefits
- Increases plant and community protection
- Improves system availability through reduced security risk
- Supplies comprehensive view of plant cyber security status
- Enhances risk mitigation against a cyber security attack
- Provides solid foundation from which to build a sustainable cyber security strategy
- Improves cyber awareness
- Enables compliance with regulatory standards
- Better IT/OT Collaboration

Controls — Security Updates, Malware Protection, Backups, Asset Inventory, Analytics, Allowlisting

Maintenance

Training

Consulting — System Hardening, Network Monitoring, Procedure and Policy

Operations — Event Monitoring

Design and deploy a strong network architecture

Likelihood of being affected: High / Low

Non targeted threats | Hobbyist hackers | Professional hackers | Nation states

Low — High

Architecture reviews

One essential step of any production system is having a well-designed network. By reviewing the existing architectural design, potential improvements might highlighted and identified to ensure that data can flow securely from and to the industrial system while remaining safe and secure. Having a secure architecture is a fundamental building block of cyber security.

Cyber security policies and procedures

Like all other "licence to operate" systems such as process safety, cyber security needs a well-defined and managed governance system. ABB can support clients with reviewing existing documentation, identifying improvements and gaps all the way through to supporting the creation of a new governance model.

OG86 gap assessments

The Health and Safety Executive have recognised the potential safety implications of a cyber attack and have produced guidelines for companies to follow. These guidelines are focused on 4 key areas, Managing Risk, Protecting against cyber-attack, Detecting cyber security incidents and Minimising the impact. ABB can undertake a gap assessment against these guidelines to identify company's strengths and weakness which will then provide the next steps along the journey.

Risk assessment

Risk assessments are a vital requirement of any cyber security management plan, as it allows companies to identify and quantify the risks which exist in their current systems. ABB can provide a range of risk assessments from an OG86 risk assessment through to an expanded IEC 62443 high level risk assessment.

—
ABB ICS cyber security
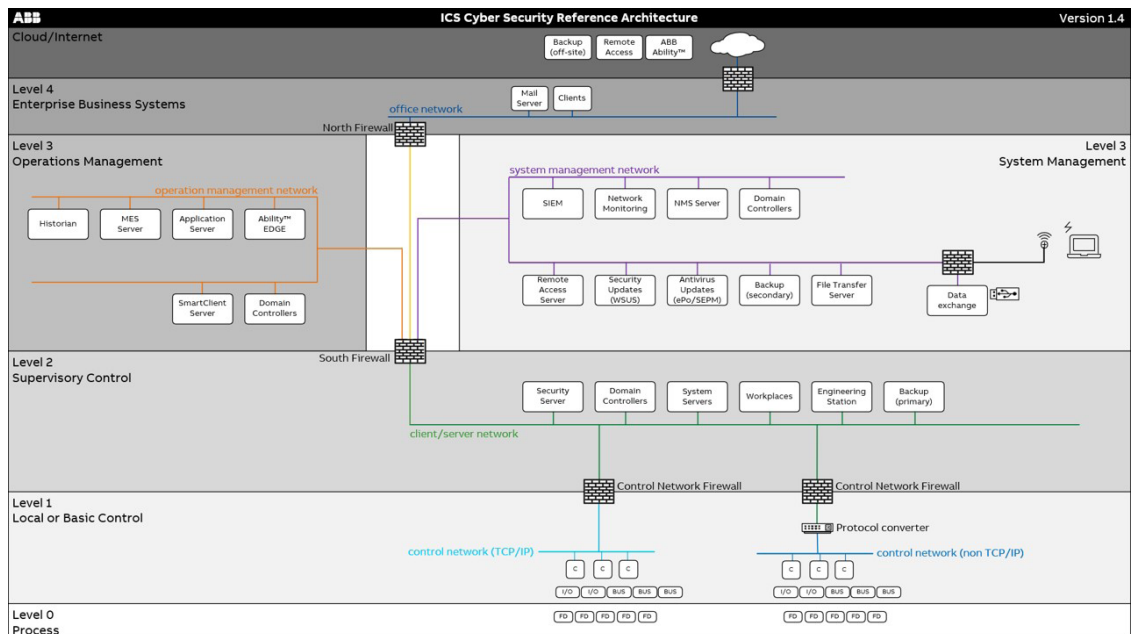reference architecture
- Overview

ICS Cyber Security Reference Architecture — Version 1.4

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

https://global.abb/group/en/technology/cyber-security