ABB Ability™ Cyber Security Assessment- Fingerprint

Protect control systems against potential security threats

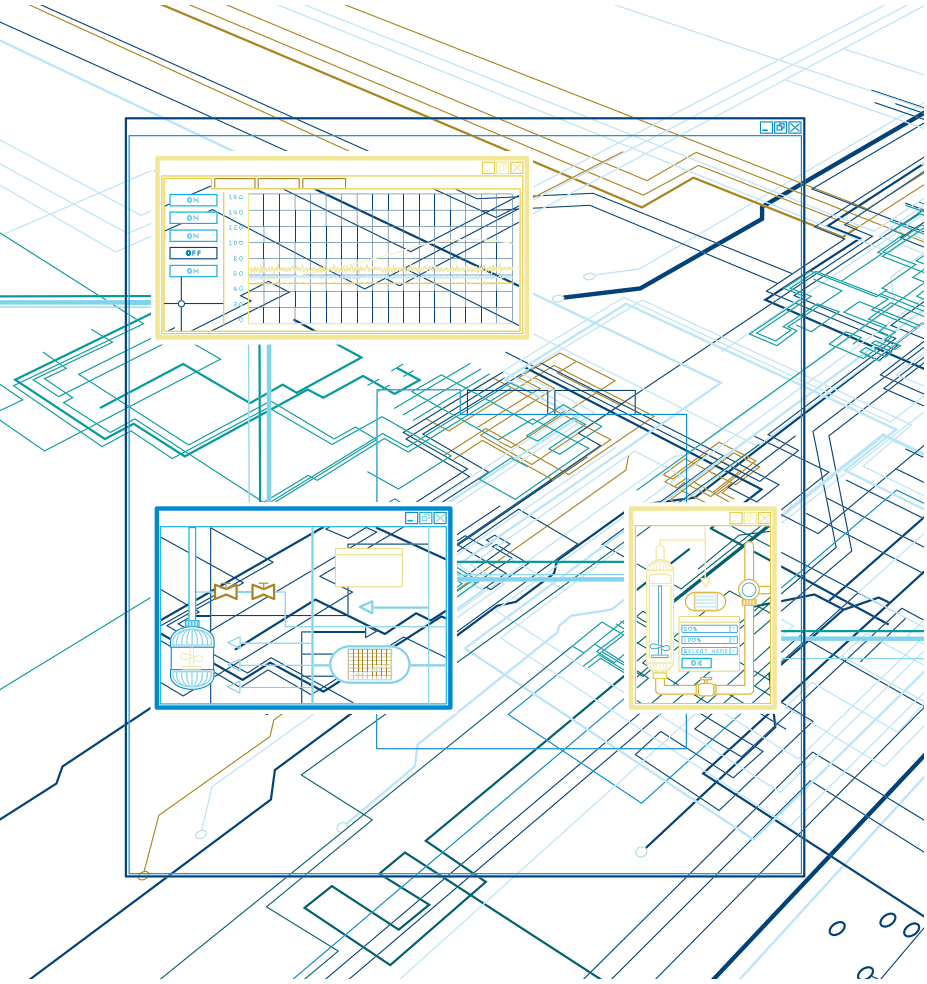


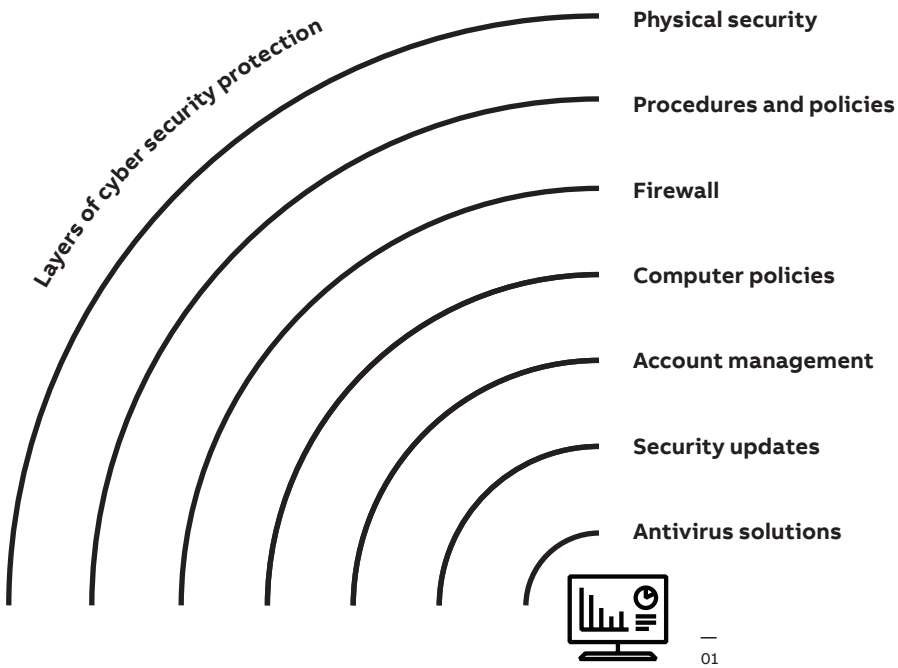
ABB Cyber Security Fingerprint identifies strengths and weaknesses for defending against a cyber attack within a plant's control systems. Key personnel use ABB's software-based analysis tool that gathers and analyzes data from critical system configurations and compares them against industry standards.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

Features:

- Based on widely used standards and best practices
- Detailed findings report with recommendations to quickly close security gaps
- Software-based analysis tool to compare plant security status to best-in-class
- Standard and repeatable process to ensure consistent analysis across systems and plants
- Sustaining services are available to regularly and proactively analyze Key Performance Indicators (KPIs)

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



—
01

All control systems are exposed to threats

Discover the vulnerabilities within your control system security

—
01 ABB uses the Defense in Depth strategy to ensure you have multiple layers of protection.

Why control system owners need to focus on cyber security

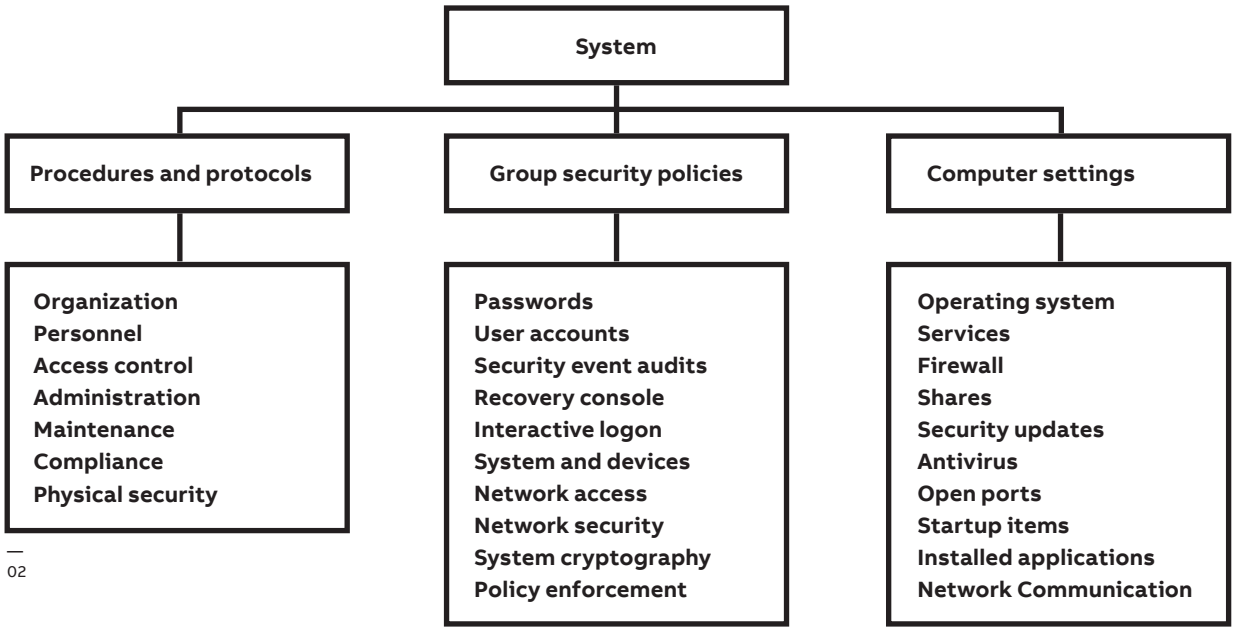
Today's industrial control systems are networked more than ever before and everyday, new risks emerge that threaten control systems security. Whether it's a malicious attack or an unintentional security breach the potential impact of such an incident could lead to endangerment of public or employee safety, loss of production, violation of regulatory requirements, harm to the environment and equipment damage.

Having a well-defined cyber security strategy can help mitigate the risk of employee or system error as well as targeted attacks. ABB Cyber Security Fingerprint reduces security risks by exposing gaps that could put employees, assets and uptime at risk. ABB's approach follows the Defense in Depth strategy and compares your security policies and settings to industry standards to ensure your control systems have multiple layers of protection (Figure 1).

Ensure you have the right protection in place

ABB Cyber Security Fingerprint is a non-invasive benchmark service that can be applied to any control system (Contact your Account Manager about your specific control system.) and consists of three-part data collection:

- ABB's proprietary high-speed, software-based collection tool, Security Logger, collects information and system settings from the control system and computers on the plant network.
- This data is coupled with information gathered from structured interviews with key plant personnel to compare system and plant security status to industry best practices and standards, such as the NERC-CIP series and ISA/IEC-62443 (formerly ISA-99).
- The Security Analyzer is then used to calculate KPIs, which highlight strengths and weaknesses of control system cyber security.



—
02

—
02 ABB examines three key components of a plant's control system to determine KPIs.

—
03 ABB generates a diagram to show a roll up of your control system's overall security status.

Key performance indicators

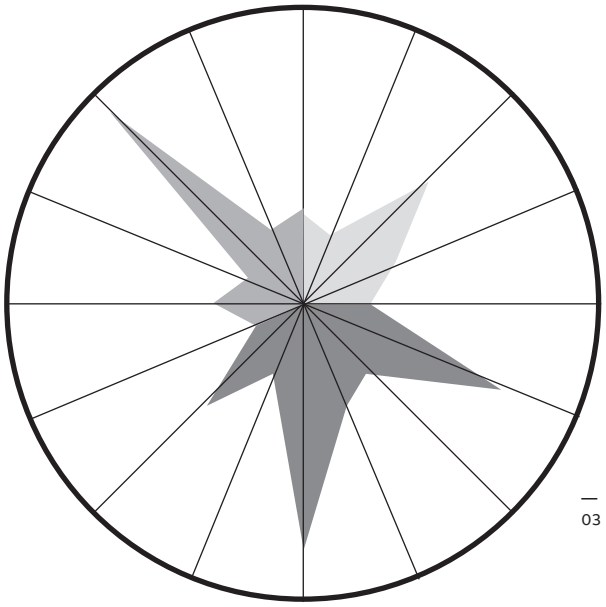
After verifying and collecting the data, ABB determines KPIs for the following areas (Figure 2):

- **Procedures and protocols:** qualitative analysis that indicates how secure the organization is by the means of written instructions and policies.
- **Group security policies:** policies implemented on the system, enforced from a central server or implemented on an individual computer.
- **Computer settings:** settings and applications that reside on individual computers in the system.

Reporting

After the evaluation is concluded, a report is generated, exposing the cyber security threats within the control system infrastructure. Based on the three areas assessed, a diagram is generated, showing your cyber security risk (Figure 3). While a small diagram indicates a low-risk environment, it does not mean the system is safe from attack. It does, however, indicate that good basic security is intact for the system, therefore reducing the risk of an attack.

The report also includes detailed findings for each section and recommendations to reduce vulnerable areas. ABB is able to assist in implementing recommendations.



—
03

Sustain security improvements
Scheduled or on-demand monitoring of KPIs

Implement and sustain

The ABB Cyber Security Fingerprint is the first step in identifying vulnerabilities within your control systems for security breaches. While the report is an indicator of your security status at a given time, recommendations do not guarantee a 100 percent secure control system. Any system, no matter how many precautions are taken, can be compromised. For best results and a consistent security level you should continue to apply several components, such as patch management and virus updates.

ABB Cyber Security Services follow a three-phase methodology to minimize process and system problems, ensure efficient operations and increase your return on assets. After implementation, ABB recommends Cyber Security Analytics Service, or scheduled or on-demand security KPI monitoring.

Contact your ABB service representative to obtain additional information or to schedule an ABB Cyber Security Fingerprint for your site.

ABB Advanced Services apply a three-phase methodology

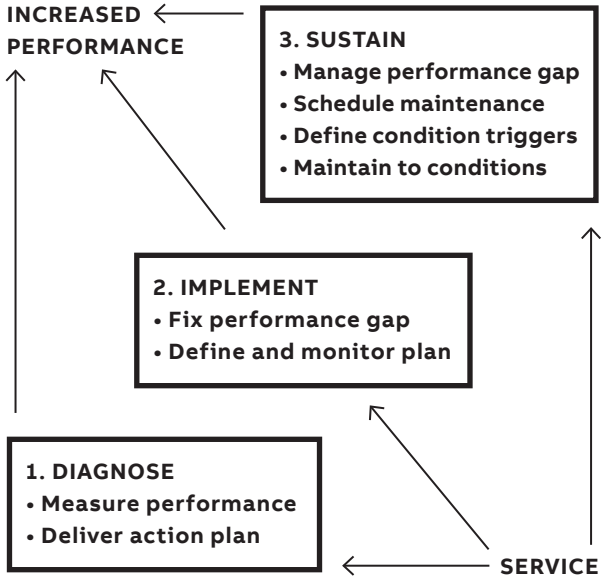


ABB Ltd.
579 Executive Campus Drive
Westerville, OH 43082
automation.service@us.abb.com

abb.com/cybersecurity

9AKK105408A9350A