POWER GENERATION

Cyber Security Solutions

Mitigating risk and enhancing plant reliability

Providing a roadmap to achieve improved reliability

In today's business environment, cyber security is critical to your plant's reliability.
ABB delivers cyber security solutions to enhance reliability, automate compliance efforts and minimize risk, tailored to the needs of our power generation customers.

In a power plant, cyber security issues can put your operations at risk. ABB can assist with solutions to meet the cyber security needs of your plant's Distributed Control System (DCS). These solutions are tailored to meet your specific requirements.They are available through services delivered through an ABB Power Generation Care contract and solutions available through ABB's Cyber Security Workplace.

With Power Generation Care, ABB delivers cyber security services to match the operational and maintenance needs of a power generation facility. We transform routine maintenance tasks and free resources to proactively focus on power production through planned delivery of updates and patches that address cyber security. ABB's DCS cyber security consulting services identify the strengths and weaknesses of your current security state, remediate security gaps and maintain a strong security program.

ABB offers a combination of assessment and remediation services that can be scheduled on a periodic or continuous basis. The assessment services include ABB's cyber security Fingerprint. Remediation services provide systems hardening, patch and antivirus deployment, and backup and restoration.

A key component of ABB's cyber security offering is Cyber Security Workplace. It is designed to meet the unique needs of the electric power industry to achieve and maintain reliability, security and compliance. Cyber Security Workplace provides an integrated suite of security applications and tools that are certified for use on the DCS and qualify for support.

Delivered as a scalable solution, Cyber Security Workplace can be phased in to meet your plant or fleet-wide security and compliance needs today while providing the platform from which to grow and expand as requirements evolve and change. Cyber Security Workplace provides a solution that supports improved reliability and automation tools to simplify efforts to comply Industrial cyber security best practices, national regulations and international standards.

In today's business environment, cyber security is critical to your plant's reliability. ABB delivers cyber security solutions to enhance reliability, automate compliance efforts and minimize risk, tailored to the needs of our power generation customers.

Comprehensive security solutions for the energy provider

Fingerprint

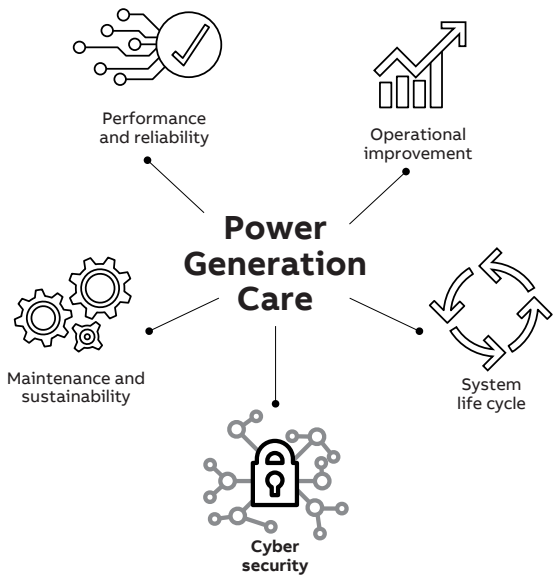
How prepared is your plant to defend your control systems from a cyber attack?

The Cyber Security Fingerprint identifies strengths and weaknesses in your control systems to defend against a cyber attack. We do this by gathering data from critical system configurations and key personnel, and comparing them against best practices. The resulting report provides detailed recommendations to reduce cyber security vulnerabilities, while helping to develop a comprehensive security strategy for your control systems.

Key features of Fingerprint include access to ABB cyber security experts, a detailed findings report with recommendations to quickly close security gaps, an analysis tool to compare plant security status to best-in-class, and a standard and repeatable process to ensure consistent analysis across systems and plants.

Fingerprint Benefits

- Provides a solid foundation from which to build a sustainable cyber security program
- Identifies opportunities for risk mitigation and increased protection against a cyber security attack
- Highlights gaps in security compliance with best practices and standards
- Delivers recommendations that lead to increased plant availability and improved safety



Security Consulting

Addressing cyber security issues in an Operational Technology (OT) environment must be managed differently than what might be common practice for IT departments.

For OT, the plant availability to produce power is highest priority.When addressing cyber security in OT, deployment guidelines, vendor validated patches and vendor validated solutions are a requirement. ABB provides both implementation, maintenance and remediation services to address OT cyber security requirements.

Our consulting services for best practices include

- Hardware & software installation, configuration & management
- Configuration change management
- Disaster recovery
- Compliance to regulations and implementation strategies
- Training for consistent maintenance of deployed cyber security solutions.
- Systems hardening
- Back-up, anti-virus and patch remediation
- Sustainability

ABB provides security assessment and remediation services before, during and after the implementation of your cyber security solutions.

ABB's cyber security solutions provide

- A single, unified view for proactive security.
- Reduced system vulnerability while increasing system reliability.
- The ability to define and monitor change management processes.
- A tool to simplify compliance in meeting cyber and regulatory security requirements (NERC CIP, IEC 62443).

Comprehensive security solutions for the energy provider

Security Patch Delivery Service

Power Generation Care delivers tested and validated Microsoft security updates and antivirus definition updates for supported ABB platforms. ABB evaluates all Microsoft security updates for relevance and system compatibility and published validation status as they are released by Microsoft.

Our security patch delivery service provides validated patches and documentation on a monthly basis. McAfee VirusScan definition file updates are included along with ABB's Microsoft security update testing. Information about the latest patch level, scan engine and validated virus definition file versions are published together with the Microsoft security update test results. These updates are available as an option with all Power Generation Care contracts.

Security Patch Delivery Service Benefits

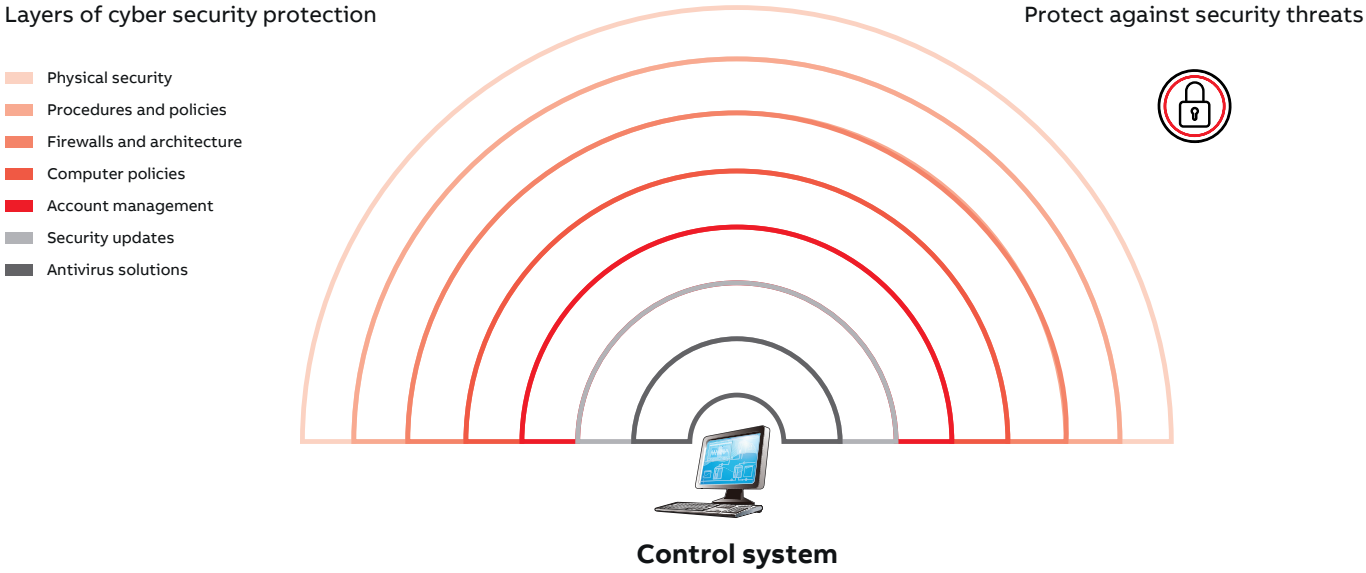
- Provides protection from intrusion and malicious software
- Closes vulnerabilities as discovered and released for Microsoft operating systems and software
- Requires no connection to the internet, update patches in an isolated environment
- Reduces the time and resources required to prepare security patch updates for your systems
- Minimizes the chance for human error in selecting approved patches
- Reduces potential for system disruptions by testing on an off-line system
- Supports security policy compliance with regulatory or corporate objectives

Security Patch Delivery Service

ABB's worldwide testing facilities download, install and qualify Microsoft patches every month. Once the new patches have been qualified, they are published in validation documents available to Power Generation Care members. When published, clean optical media (DVD) is delivered that includes all the patches sorted by each product and platform required for that month. This can be imported into the ABB Cyber Security Workplace Patch Management Utility (PMU) which centrally manages and distributes patches to ABB machines.

Protect control system
Scheduled or on-demand monitoring of KPIs

Automation security



—
01

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

Scheduled monitoring and analysis quickly identifies performance issues
The ABB Cyber Security Monitoring Service is a service delivery platform conveniently deployed at customer locations. View data through a user interface that is easily accessible by customer or ABB personnel.

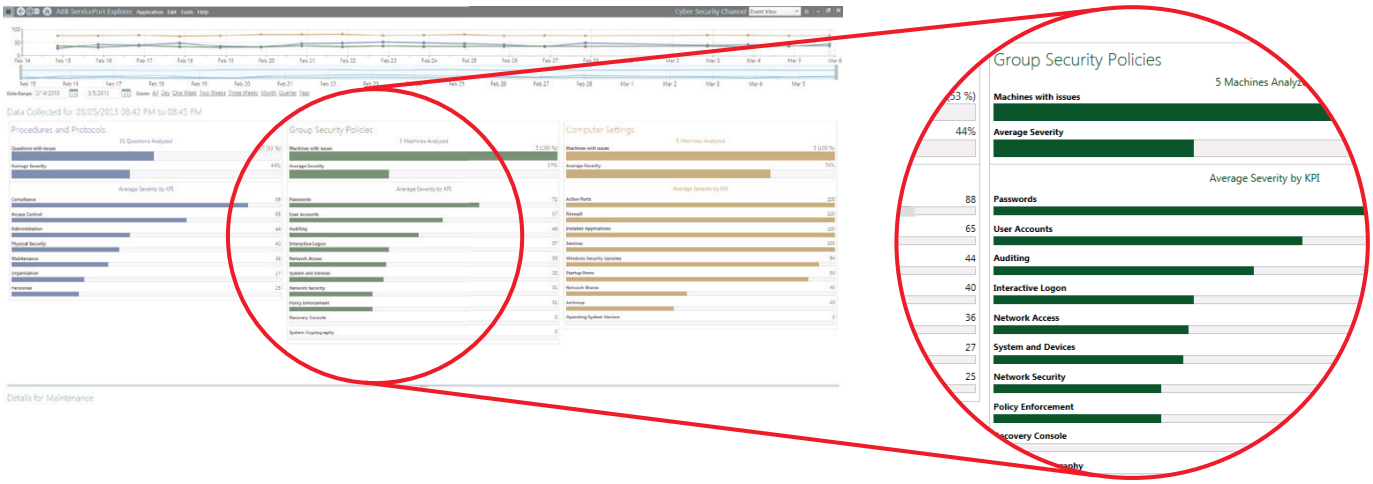
The ABB Cyber Security Monitoring Service provides proactive data analysis to greatly reduce time and effort needed to identify software, hardware, system and network performance issues. Data is classified according to KPIs to provide a list of potential issues that are then prioritized based on severity, criticality and/or financial impact. This analysis allows users to track and trend performance more accurately, which leads to more informed decision-making and higher availability, as well more easily ensuring that multiple layers of protection are in place (Figure 1).

More accurate troubleshooting with configurable KPIs
The ABB Cyber Security Monitoring Service analyzes the following KPIs (Figure 1) to accelerate problem-solving:

- **Procedures and protocols:** Availability of, and agreement with, written instruction and policies.
- **Security policies:** Compliance with policies implemented on the system, enforced from a central server or implemented on an individual computer.
- **Computer settings:** Assurance that the appropriate settings and applications reside on each computer in the system.

View, analyze and receive alerts on security status

Cyber Security Monitoring Service components



—
01

—
01 Users can access three different views for each KPI. The above example shows the KPI analysis view for security policies. The display only shows KPIs that are outside their threshold and prioritizes them: the bigger the bar, the greater the probability that the KPI should be addressed.

Clear view of data and analysis
Access and visualization of KPIs is provided through the KPI dashboard. This easy-to-use interface offers three separate views of the data:

- **View:** Raw data allows customer and ABB service personnel to view data associated with Security and performance for further analysis.
- **Scan:** Automatic KPI analysis presents a summary of KPIs, ranked by severity, that are outside set limits, so that users can begin addressing issues in order of priority.
- **Track:** Users can specify sets of rules for KPIs and display each occurrence that falls outside a threshold, so that users can be proactively notified to address issues.

Expert analysis helps predict potential weaknesses
To ensure that your cyber security status is aligned with your security goals, ABB provides periodic performance analyses. ABB experts evaluate the status of your system's security level, determine the statistical accuracy of KPIs and find trends that predict potential vulnerabilities. The resulting performance report recommends actions to improve procedures and protocols, system policies and computer settings.

Critical notification when it matters most
To prioritize issues that require immediate action, site-specific rules can be applied to targeted KPIs. Any KPI that tracks outside customizable, pre-determined parameters triggers an instant alert via email or text message. This quickly notifies users about issues that can compromise security, so they can be addressed as soon as they are detected.

Removable media risk mitigation

—
01 Process for trusted file transfer

The risk: "trusted files from trusted insiders"
A common cyber security threat in any power plant or operational environment is the trusted insider or contractor who unintentionallys introduces malicious software, or malware, by means of an infected file or USB firmware transferred through removable media. Control systems are open to attack whenever someone imports files into an Operational Technology ("OT") environment from any source. Malware is designed to evade anti-virus scans and other common detection technologies and to stealthily execute its mission. When essential software or security patch updates are required, how can a plant trust it to be safe? All sources and files should be considered untrustworthy.

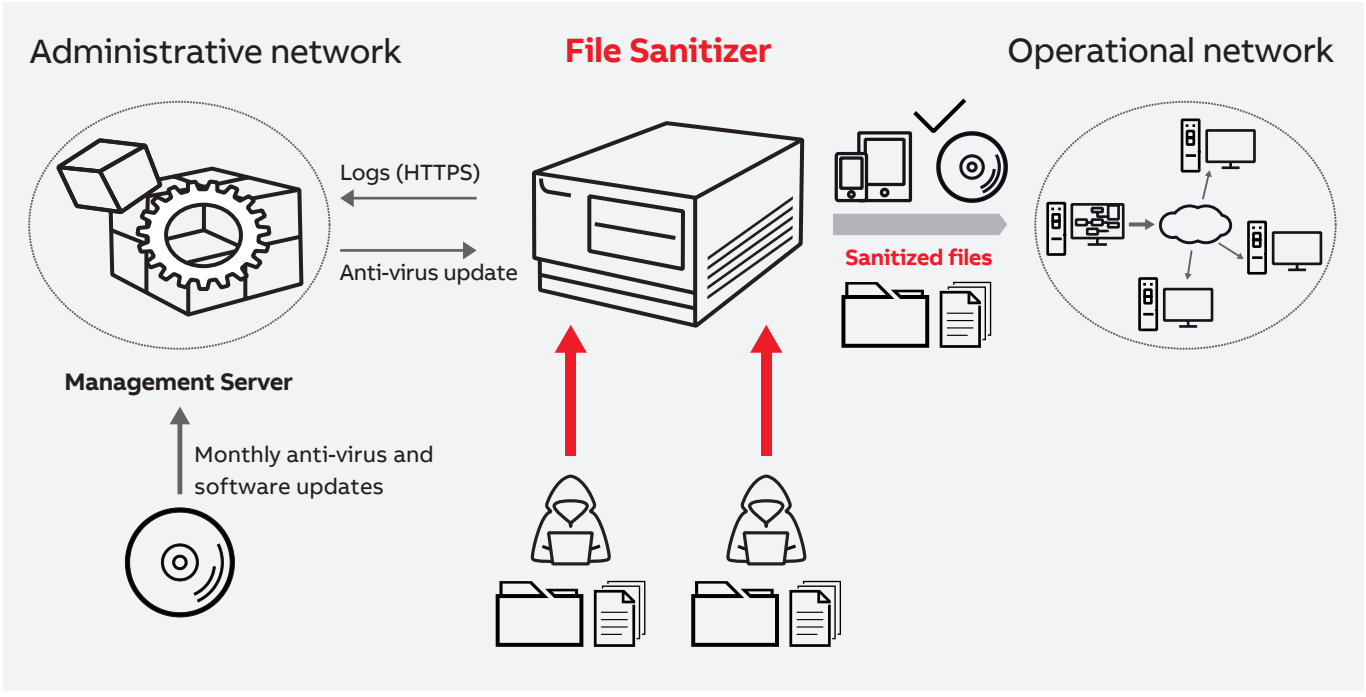
The Solution: Cyber Security Workplace File Sanitizer
To mitigate the risk from introducing an infected file into your OT environment, ABB provides the File Sanitizer that neutralizes and removes undetectable malware. ABB uses a multi-stage sanitation process that rapidly produces trusted files. This proprietary method is the only proactive approach in use today that does not rely on detection or identification.

The File Sanitizer can be deployed in an air-gapped environment or connected to the plant network and centrally managed. Depending upon the desired architecture, the sanitized files can be transferred to read-only media (CD-ROM) using a trusted USB drive or to a file server. The File Sanitizer provides a controlled environment where physical devices can be inserted into the system (meets NERC CIP v5 CIP-010-2 R4). This hardened appliance is resistant to any attack and will process all selected files from the removable media and deliver only those that have been sanitized.

ABB recommends only files that have gone through the File Sanitizer be introduced to the DCS via trusted media or networked file transfer from the File Sanitizer.

File Sanitizer features and benefits
- Unique process based on proprietary algorithms.
- Sanitizes all files from known and unknown malware.
- 5 different anti-virus engines.
- Sanitizes all files from known and unknown malware.
- Operating system hardening: the File Sanitizer boots from a LIVE CD.

—
01



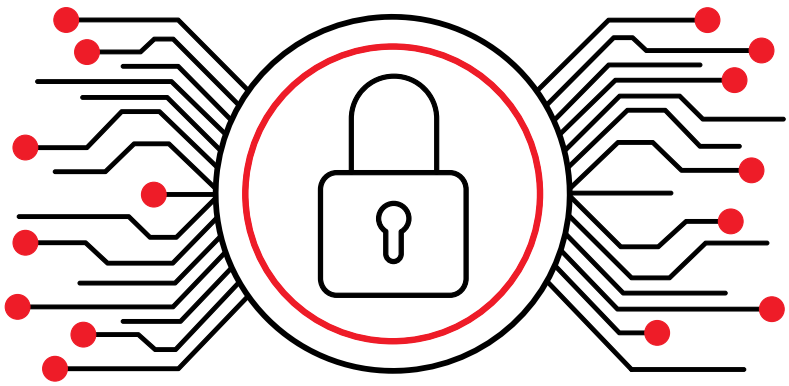
Cyber Security Workplace
Reliability – Security – Compliance

The reliable operation of your ABB Distributed Control System (DCS) depends on your ability to DEFEND the ABB recommended security baseline for the networking and computing platforms that comprise the system. Un-patched servers and clients with outdated consoles are very soft targets. They can be easily compromised and adversely affect the reliable operation of the DCS.

To meet the OEM recommended security baseline, ABB provides the Cyber Security Workplace PROTECT solution. These applications and services have been validated for your ABB DCS.

Cyber Security Workplace Protect includes
- System and network hardening
- Security patch delivery disk
- Centralized Microsoft patch management
- Centralized anti-virus management
- Automated back-up and recovery

ABB Cyber Security Workplace



System and network hardening
Server and workstation hardening secures a system by reducing its surface of vulnerability. A system has a larger vulnerability surface the more functions it fulfills.

ABB limits the amount of functions and communications as much as practical for the control system to operate as intended. ABB applies basic server and workstation hardening profiles based on the operating system, DCS system, and third party software of the machines.

Centralized Microsoft patching management
The deployment of tested, validated Microsoft patches for your ABB DCS is greatly simplified using the Patch Management Utility (PMU): The time required to manually deploy Microsoft patches to your system is reduced by up to 75%. The PMU works directly with the Power Generation Care cyber patch delivery DVD to allow an air-gap functionality within the DCS network. No Internet connection is required.

Cyber Security Workplace delivers fleet-wide security solutions for ABB and multi-vendor control systems. The amount of risk posed to your operation from an intentional or accidental cyber related incident will depend on your organization taking a measured response today to the escalating threats coming at you tomorrow. Cyber Security Workplace provides a scalable solution to address your needs for reliability, security and compliance.

Cyber Security Workplace
Reliability – Security – Compliance

PROTECT

- Cyber security Fingerprint Patch Management
- Malware Protection Management
- System Hardening
- Backup and Restore Management

Basic, reactive countermeasures to protect against the most common threats

DEFEND

- Cyber security Assessment
- Cyber Asset Management
- Patch Management
- Malware Protection Management
- System Hardening
- Backup and Restore Management
- Network Security Management
- User and Access Management
- Security Monitoring (Basic)

Advanced countermeasures to protect against the most common threats, including foundations of a systematic security management system

MANAGE

- Cyber Asset Management
- Patch Management
- Malware Protection Management
- System Hardening
- Backup and Restore Management
- Network Security Management
- User and Access Management
- Security Monitoring (Advanced)
- Disaster Recovery/Emergency Response
- Compliance Management
- Incident Response
- Threat Intelligence

Comprehensive countermeasures to protect against advanced and emerging threats, comprehensive security management system including compliance management/ reporting

Power Generation Care contract

Cyber Security Workplace: PROTECT

Achieve and maintain the ABB recommended security baseline to meet the basic requirements for continued reliable operation of your ABB DCS. Using ABB approved automation tools to manage the essential patching and back-up processes insures the accuracy and consistency needed to maintain a security baseline.

Cyber Security Workplace: DEFEND

By being proactive in regards to security and systems management, you will gain the necessary visibility into the DCS to identify and correct conditions that threaten reliable operations. A single pane of glass or “dashboard” will allow you to monitor the health of your DCS and view security events, configuration changes and alerts regarding thumb drive use. Without these measures, the first indication there is a problem with your DCS will be when the system goes down and your plant trips.

Cyber Security Workplace: MANAGE

Provides a common reporting structure and an integrated approach to managing all compliance requirements faced by an organization, allowing you to focus on system reliability and performance – not compliance paperwork. Policy management, automated data collection and built-in standard reports drastically reduce the preparation time required for compliance audits.

ABB Inc.
Industrial Automation – Power Generation
Wickliffe, Ohio, USA
Phone: +1 440 585 7804
E-mail: pspmarketing@us.abb.com

ABB AG
Industrial Automation – Power Generation
Mannheim, Germany
Phone: +49 621 381 33 33
E-mail: powergeneration@de.abb.com

ABB Pte. Ltd.
Industrial Automation – Power Generation
Singapore
Phone: +65 62 22 77 78
E-mail: powergeneration@sg.abb.com

ABB
Industrial Automation – Power Generation
Abu Dhabi, AE
Phone: +971 2 493 80 00
E-mail: powergeneration@ae.abb.com

ABB Co.
Industrial Automation – Power Generation
Beijing, China

ABB
Industrial Automation – Power Generation
Northern Europe
(UK, Denmark, Norway, Sweden, Finland)
E-mail: FI-IAPG-NorthernEurope@abb.com

ABB Pty
Industrial Automation – Power Generation
Modderfontein, South Africa

ABB S.p.A.
Industrial Automation – Power Generation
Genoa, Italy
Phone: +39 010 607 3512
E-mail: powergeneration@it.abb.com

abb.com/powergeneration

2VAA006744 Power Generation October 2017 en