ABB Advanced Services

I am protection for your system
We are cyber security services

Connected automation systems are making utilities and industry more efficient, more productive, and more economic, but they are also introducing new challenges to those organizations.

The visibility and control provided by semi-autonomous systems can render utilities and industrial applications vulnerable to cyber attacks, requiring a new kind of defence.

ABB fully understands the importance of cyber security and its role in advancing the security of substation automation systems. By investing in ABB technologies, you can be sure that reliability and security of your systems have been given the highest priority. ABB's cyber security portfolio helps you to mitigate the risk and potential impact of a cyber attack.

Offering includes

- Cyber security assessment
- Perimeter protection
- Malware protection
- Patch management
- Back-up and recovery
- Intrusion Detection and Prevention Systems (IDPS)
- Security monitoring
- Product and system hardening
- Vulnerabilities information and updates

Benefits include

- Identification of vulnerabilities of systems and organizations
- Enhanced plant and network protection
- Improved system availability though reduced security risk
- Comprehensive view of security borders
- Risk mitigation against cyber attack
- Improved confidence in the security of the systems
- Configuration back up, ensuring faster recovery, should an incident occur

Power and productivity
for a better world™

We help you protect your system
Assess - Implement - Sustain

With a complete view of the network, it becomes possible to identify points where additional security should be applied. This will come in a variety of forms, beginning at the borders and extending into every part of the network.

Perimeter protection
Firewalls can protect the perimeter of a network and a well-designed security policy will separate the network into distinct, controlled zones, protected by internal firewalls to ensure that a compromised server doesn't mean compromise the entire network.

Malware protection
Our systems can be equipped with industry-standard malware and intrusion protection solutions, like anti-virus protection and application whitelisting.

Patch management
It's not just the anti-virus software that needs modern operating systems and embedded software often need to be patched to defend against emerging threats. Efficient patch management is an essential part of any security policy, but one that is often neglected.

Back-up and recovery
If the worst does happen, and cyber attack or natural disaster strikes, then the security of an off-site back-up will make recovery that much easier. ABB's back-up solutions can ensure the integrity, and availability, of critical data, no matter what happens to the original.

Intrusion Detection and Prevention Systems (IDPS)
IDPS are network security appliances that monitor network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

System Data Management
ABB's System Data Manager (SDM600) is designed to track versions and configurations of software embedded in IEDs (Intelligent Electronic Devices), and provide visibility of security alerts, which may indicate an attack in progress.

SDM600 also manages user accounts across devices, keeping track of users and their access privileges. User accounts are a critical part of cyber security. The vast majority of cyber attacks are carried out by hackers using legitimate credentials, stolen or guessed, so it is vitally important that access privileges are regularly reviewed. expired accounts are promptly deleted, and users are given access only to those areas they really need to use.

Implement and sustain
The ABB Cyber Security Assessment is the first step in the process of identifying vulnerabilities within your control systems. While the Assessment report provides an indication of your security status at a given time, its recommendations do not guarantee that your system is a 100 percent secure. Any system, no matter how many precautions are taken, can be compromised. For best results and a consistent security level, several components, such as patch management and virus protection, should be applied and regularly updated.

ABB Advanced Services follow a three-phase methodology (Figure 1) to optimize processes and systems, ensure efficient operations and increase your return on assets. After implementation, ABB recommends that you enter into a Service Level Agreement, which provides you with selected cyber security offerings to ensure that reliable operations can be maintained.

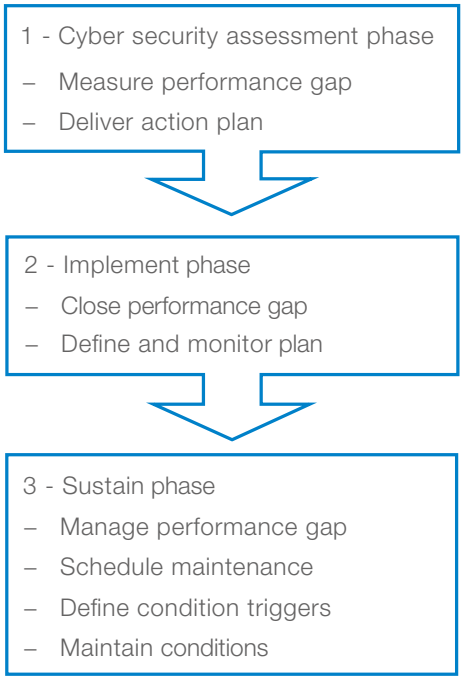

Figure 1: ABB Advanced Services apply a three-phase methodology.

Cyber security isn't a single problem, with one solution. It's an on-going battle, and ABB provides a range of products and services that can help protect your network, and the equipment connected to it from the evolving threats emanating from the world.

Let us assess your system
We are cyber security and service at your fingertips

Cyber Security Assessment

For ABB, the process of cyber security management starts with a Cyber Security Assessment: a detailed analysis of existing systems and possible points of weakness. The ABB Cyber Security Assessment brings ABB experts to the customer site, to interview staff and inspect equipment and assess procedures in use. That process takes a few days, and is followed by several days of analysis to build a comprehensive assessment of the existing configuration.

The result of an ABB Cyber Security Assessment is a detailed report comparing the tested installation against industry best practice and standards, including NERC-CIP series and ISA/IEC-62443 (formerly ISA-99). The Security Analyzer is then used to calculate key performance indicators (KPIs) to highlight strengths and weaknesses of control system cyber security.

The process can be repeated, so the impact of subsequent improvements to security can be accurately measured over time. At this stage, many customers take advantage of ABB's Cyber Security Monitoring Service for scheduled or on-demand security; KPI monitoring on an ongoing basis.

Assessment delivery schedule (schedule dependent on size of system installation.)	
Day 1	Project introduction meeting
Day 2	Begin collecting security data Interview key plant personnel Make configurations accordingly
Day 3	Complete process data collections Data analysis begins Exit meeting
Day 4-5 (off site)	Complete data analysis Prepare summary of findings

Key performance indicators

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

- Procedures and protocols: of written instructions and policies to assess their contribution to the security of the organization.
- Group security policies: policies implemented on the system on an individual computer, or enforced from a central server.
- Computer settings: settings and applications that reside on individual computers in the system.

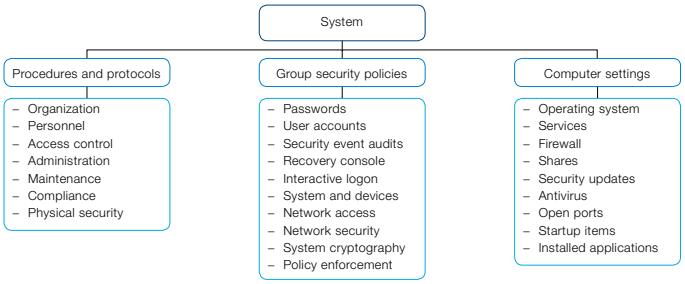

Figure 2: ABB examines three key components of a plant's control system to determine KPIs.

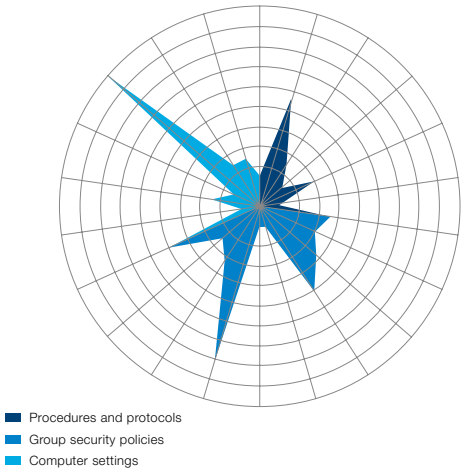

Figure 3: ABB generates a diagram to show a roll up of your control system's overall security status.

Why is cyber security so important?

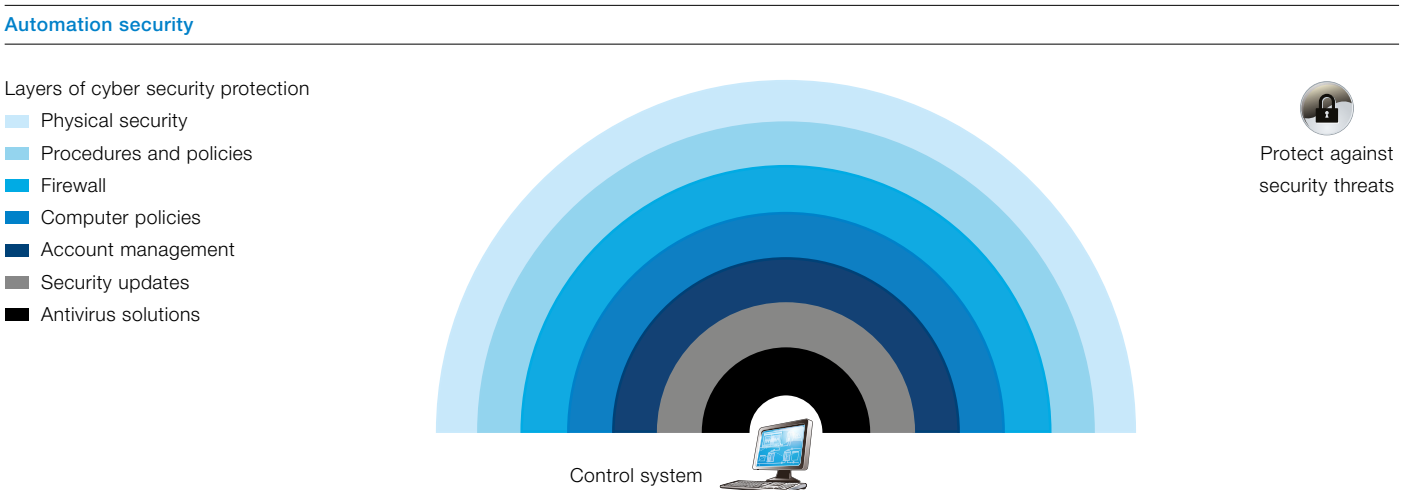

Figure 4: ABB uses the defense-in-depth strategy to ensure multiple layers of protection.

Could your cyber security strategy be more robust?

Having a well-defined cyber security strategy can help mitigate the risk of employee- or system-based error, as well as targeted attacks. We are your strategic partner for mitigating cyber security risks.

We are your cyber security partner

The best way to secure a network is to enforce good practice with specialist hardware and software protection systems to minimize the risk of external attacks.

Understand your installation and invest in expert recommendations

Security is no longer an all-or-nothing proposition, where attackers are held back by impenetrable gates. It is a holistic and ongoing process with layers of protection ensuring that critical systems are protected from both internal and external threats..

Contact your local service and sales support team to discuss your requirements.

For further information visit:
http://new.abb.com/network-management/service

4CAE000023 Rev-