ABB Ability™ cyber security services

Protect your control systems from the threat of cyber-attacks
Overview

In today’s business environment, cyber security is critical in ensuring reliability of Industrial Automation and Control Systems (IACS).

All organisations should establish a Cyber Security Management System (CSMS) to effectively understand and mitigate cyber risk. A CSMS is an excellent process for managing risk within a large and complex organisation, but it is equally effective within smaller companies too.

ABB have developed a range of cyber security services which help organisations of all sizes establish and maintain a CSMS which is tailored to their specific needs and risk appetite.

Threats to industrial systems
Industrial control systems are changing. Organisations are harnessing the wealth of information available throughout their industrial control systems to make them more competitive. This has led to more interconnected systems which results in greater exposure to cyber threats.

Targeting of safety systems
In late 2017, we saw the first publicly known cyber attack to specifically target human life. The TRITON / TRISIS malware targeted the Safety Instrumentation Systems (SiS) of a Petrochemical plant in the Middle East and has since been reported attempting similar attacks on other systems around the world.

Ransomware attacks
The number of cyber attacks on control systems is increasing. Industrial systems are an attractive prospect for cyber criminals. They know that if they can stop production, paying a large ransom is an option likely to be considered if the alternative is to lose significantly more through loss of production, recovery costs and reputational damage. Companies increasingly need to ask themselves - if we were held to ransom whilst your production has stopped, would we be able to respond effectively?

Industrial espionage
Industrial espionage is nothing new, but cyber attacks are making this activity much easier. Criminals are motivated to steal intellectual property from competitors in order to gain an advantage. Attackers have realised that control systems contain a wealth of valuable information right down to the field level of a plant which could be used to gain a commercial advantage over their victim. The UK government estimates that £7.6bn is lost to cyber industrial espionage each year.
All organisations are required to manage their cyber security risk to ensure their continued success.

ABB have developed a comprehensive set of cyber security services which are based on industry best practices on the development, implementation, operation, maintenance and assessment of a Cyber Security Management System (CSMS). Each service can be easily tailored to meet the specific needs of any organisation we work with.

The diagram below shows the process of a CSMS and how each of our services can help with each step.

At ABB, we realise that traditional cyber security approaches don’t work when it comes to industrial control systems:

- Locking out accounts after 3 failed password attempts would mean an operator has no control over the process for a period of time
- Use of cryptography to protect data in transit could mean time constraints aren’t met in control system communications
- Many intrusion detection systems don’t speak the digital communications technologies of HART, IEC 60870-5-104, OPC or IEC 61850
- A malicious command to shutdown plant equipment would look identical to a legitimate command. You must use pattern of life analysis to identify malicious activity of this type

We have developed services that cater to the specific needs within industrial systems.
Identify

Asset management
To ensure you fully understand what you need to protect we can help you create and maintain an accurate inventory of automation assets within the operational environment.

Cyber security risk assessments
Our risk assessments follow best practice processes to assess the cyber risk to your organisation. By using this service you will have a solid understanding of the current risk level within your organisation and have a clear plan on how to mitigate these risks. Improve security of your automation control systems by performing a threat / risk-based assessment.

Gap analysis
We can assess your organisation’s cyber security management system against industry best practices and standards and identify areas for improvement.

Vulnerability assessment
In order to fully understand the cyber risk to your organisation, ABB can carry out periodic vulnerability assessments to identify where different vulnerabilities lie within your system.

Penetration testing
Penetration testing is a great way to identify security vulnerabilities in your organisation. Carrying out a simulated attack on industrial control systems not only identifies vulnerabilities within your system, but also identifies how these vulnerabilities can be exploited, so you can better understand what security controls to put in place to mitigate or remove these vulnerabilities in your system.

Open Source (OS) intelligence
The first stage of a cyber-attack is reconnaissance. This is where the attacker will gather as much data as possible about potential victims as possible. We can carry out this process to identify what a potential attacker can find out about your organisation before they do. The output of this process will often identify confidential information accessible on the internet, internet accessible industrial devices and potential targets for phishing emails.

Protect

Malware protection management
Ensure effective protection from malware by having protective technology deployed on end-point assets.

Security patch management
Reduce the likelihood of a successful cyber-attack by regularly implementing software patches on automation systems.

System hardening
Reduce the risk of a cyber-attack by examining the configuration settings, policies and removing or deactivating software, services, user accounts and open ports.

System backup and recovery management
In the event of a system failure, it is of the utmost importance that you have a robust backup system that can provide system restoration in the event of an incident to ensure business continuity.

User and access management
Ensure that users of the system always have the approved and relevant access rights.

Cyber security training
We offer a range of cyber security awareness courses that will ensure employees are aware of the role they play in the security of their organisation.

Detect

Intrusion detection and analysis
We can help you look for and detect malicious activity, security vulnerabilities and best practice improvements within your system.

Respond

Incident response
We can help you with the preparation and implementation of your organisation’s incident response plan to ensure your response to cyber incidents ensures minimal impact.

Cyber exercising
We can provide real life scenarios that test your people, processes and technology in protecting your system from the threat of cyber-attack, identifying critical lessons learnt to identify ways to make your system more secure.

Malware analysis
In the event that malicious software is found on your system, we can use our specialist knowledge of industrial control system specific exploits to carry out analysis which will help you determine the functionality, origin and impact of each piece of malicious code.

Recover

System restoration
We can help you bring your system back online in the event of an incident. Attempting to recover without planning and preparation can cost more than five times as much.
Why ABB Ability™ cyber security services

We bring three key areas of expertise:

**Technology**

ABB pioneered the development of electrical and automation technologies, and has years of experience helping customers protect control systems and other automation assets. Our cyber security solutions are aligned with industry standards and go through rigorous testing before they are released.

**Industry knowledge**

ABB’s control systems are present globally across many industries. We know the type of cyber threats our customers face and what needs to be done to mitigate risks. We stay ahead of threats by investing heavily in research and development to continuously improve our security offerings.

**Analytics**

ABB has been helping customers become more cyber-secure through strong data analytics and visualisation. Our technology identifies, categorizes and prioritises Key Performance Indicators (KPIs) automatically, so our experts can determine the best risk mitigation strategies.

---

**Case studies**

**Refinery, Middle East**
Ensuring that comprehensive cyber security policies and procedures were applied across its process control systems.

*We met that need with*
- The plant used the ABB Ability™ Cyber Security Fingerprint to review existing security measures and identify security gaps

*Customer benefit*
- Comprehensive view of plant cyber security status
- Better risk mitigation against a cyber-attack
- Tighter security procedures

**TANAP Pipeline, Turkey**
1800KM gas pipeline project across Turkey. Integrated security system to protect critical infrastructure.

*We met that need with*
- Cyber security system design, assessment, hardening and monitoring

*Customer benefit*
- Integrated security system in line with industry best practice. Early detection and mitigation of potential attacks

**Pulp and paper mill, Germany**
Needed to improve cyber security measures for mitigating cyber risks and ensuring compliance with European Union’s security standards.

*We met that need with*
- ABB Ability™ Cyber Security Analytics

*Customer benefit*
- Reduced vulnerabilities and provided a sustainable security strategy for mill’s control systems
Make your assets cyber secure today
To get started or learn more, please contact your local ABB sales representative or visit:

abb.com/cybersecurity