A vital step in ensuring your assets' security — ABB Ability™ cyber security gap assessment

A vital step in ensuring your assets' security
In today’s business environment, cyber security is critical to ensuring the safe and reliable operation of Industrial Automation and Control Systems (IACS). Legislators and regulators have decided to enforce companies to take action and to provide evidence that protective systems are in place to mitigate the risk of a cyber-attack causing harm. To identify, understand and mitigate cyber security risks, all organisations should have implemented an ongoing Cyber Security Management System (CSMS). A CSMS is an excellent way to manage risk within a large and complex organisation, but it is equally effective within smaller companies too. ABB offer a wide range of cyber security services to help organisations of all sizes establish and maintain a CSMS, tailored to their specific needs and risk appetite.

An ABB Ability™ cyber security gap assessment is an essential step to ensuring your company implements an effective CSMS. By identifying areas of your current CSMS that result in increased risk exposure, or non-compliance to regulatory and legislative requirements, problematic areas are identified and can be fixed. ABB understands that no two businesses are the same, as such we offer a highly customisable service. Our gap assessment can be tailored to your exact needs by considering the legislative requirements of your country of operation and any other standards you require compliance with.

European Union (EU)
The Network and Information Systems (NIS) directive
The NIS directive is a EU wide legislation that seeks to raise the overall resilience of the EU to cyber security threats on critical infrastructure. The deadline for transposing into law for each member state was May 2018, so the NIS directive is now a legal requirement in every EU country. The NIS directive applies to all network and information systems that are deemed to be ‘Operators of Essentials Services (OES)’, for example utilities or healthcare.

Non-compliance with the NIS directive leads not only to unacceptable business and safety risks, but could also lead to hefty penalties, with a maximum fine of £17,000,000 being possible. Applicability of the NIS directive is not limited to OES. ABB can perform a gap assessment on your company’s CSMS whether you are an OES or you wish to be held to the same standard to reduce business and safety risk.
The UK’s National Cyber Security Centre (NCSC) developed the CAF as a tool for competent authorities to assess OES against the requirements of the NIS directive. If you are an OES then compliance with the CAF is mandatory and non-compliance can result in a fine. A gap assessment against the CAF framework can also be beneficial for operators of assets who wish to adhere to the same strict standard to mitigate business and safety risks posed by a cyber-attack.

The UK HSE’s operational guidance 86
If your site is exposed to major hazard risk, for example COMAH sites, you are required to demonstrate that you are effectively managing your cyber security risk. The HSE have published Operational Guide 86 (OG86) based upon industry standards such as ISO27001, IEC 62443 and the CAF to guide operators on how to implement a management system to manage your risk. For those operating a COMAH site, compliance with OG86 is a mandatory requirement and the HSE are routinely inspecting sites for compliance. ABB has significant experience and expertise in this field and offers a comprehensive gap analysis to aid your company in becoming compliant with OG86.

International Electrotechnical Commission (IEC) 62443
IEC 62443 is a series of requirements and best practices related to cyber security of IACS. IEC 62443 provides a comprehensive framework for all aspects of a network relating an IACS. Multiple countries, such as the UK with OG86, have implemented legislation based upon IEC 62443. A gap assessment against IEC 62443 is therefore an excellent choice for companies who wish to assess their assets against an internationally recognised standard for cyber security.

National Institute of Standards and Technology (NIST) framework
The NIST framework sets out a series of standards, guidelines and best practices relating to cyber security. Like IEC 62443, this framework sets out industry best practices for cyber security of industrial control systems. By having ABB carry out a gap assessment against this framework an organisation will have excellent awareness of how their cyber security management compares to that of industry best practice recommendations and allow you to identify areas where you may need to make improvements to reduce your cyber security risk to an acceptable level.
ABB ABILITY™ CYBER SECURITY GAP ASSESSMENT

Capabilities

ABB has deep domain knowledge and expertise in cyber security for the OT environment. ABB has established itself as an industry leader across all sectors in industry from oil, gas and chemicals, to pharmaceuticals, water and power generation and distribution. From the motors and drives that keep fluids flowing to our consultants who provide insight into plant operation and safety, ABB continues to bring innovation to the industry.

Two-way communication between team members across our sectors helps our teams continually evolve and innovate, in the context of cyber security this means our consultants are not only industry experts in their respective fields but have unrivalled access to experts across all sectors of the oil, gas and chemicals industry.

This means our consultants have a deeper understanding of plant operation and can go beyond just an implementation of industry standards. ABB’s unique position and history in the cyber security market means our consultants have access to proprietary tools and techniques developed throughout our global divisions.

Choosing ABB for your cyber security needs is not just putting trust in our local industry leading experts, but the expertise and experience of our consultants spanning the globe.
Benefits to clients / customers

The purpose of a gap assessment is to give you an understanding of areas of non-compliance to a technical or regulatory standard, this has obvious benefits in terms of becoming compliant to that standard. However, the benefits of a gap assessment extend well beyond this. Whilst it is important to understand areas of non-compliance, the results of a gap assessment give an overall awareness of an asset’s security.

An ABB gap assessment will go further than identifying your non-compliance by also identifying what work is required to achieve compliance and how to carry out the work in the most efficient, effective and cost effective way.

Our cyber security service portfolio: The complete life cycle of cyber security services.

- Cyber security benchmark
- Cyber security fingerprint
- Cyber security risk assessments
- Cyber asset management
- Gap assessments
- Vulnerability assessment and penetration testing
- Threat Intelligence

- Malware protection
- Security patch management
- System hardening
- Backup and recovery management
- User and access management
- Network segmentation
- Cyber security training

- ServicePort™ security monitoring
- Cyber security monitoring service
- Network security monitoring

- Incident response
- Cyber exercising
- Malware analysis

- System restoration
- Disaster recovery
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 an ABB cyber security assessment 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 cyber security assessment

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