WHITE PAPER

Cyber Security for ABB Drives

White Paper

Cyber Security for ABB Drives

Table of contents

© 2023 ABB Oy.
All Rights
Reserved.

3AXD10000492137 Rev C
EN
EFFECTIVE: 2023-04-14

Table of Contents

White Paper **3**

Introduction to the guide **7**
- Contents of this chapter 7
- About this guide 7
- Disclaimer 7

Cyber security essentials **9**
- Contents of this chapter 9
- Introduction 9
- Cyber security in automation applications and networks 10
- Cyber security and safety 11
- Cyber security regulations and standards in automation 12
- Defense in depth 14
- Roles and responsibilities 16
- Defense in depth - generic cyber security policies and controls 17
- Generic cyber security solutions in product life cycle 21
- Visualized defense in depth layers 23

Example cases **25**
- Contents of this chapter 25
- Introduction 25
- Case 1 – Industrial automation example (factory environment) 26
- Case 2 – Remote pumping stations 30
- Case 3 – Machinery OEM Equipment 31
- Case 4 – Building automation 33

ABB cyber security policies **36**
- Contents of this chapter 36
- Principle 36
- Device Security Assurance Center (DSAC) 38

Appendices **40**
- Glossary 40
- List of references 43
- Further information 44
  - Product and service inquiries 44
  - Product training 44
  - Providing feedback on ABB manuals 44
  - Document library on the Internet 44
- Contact us 45

1

Introduction to the guide

Contents of this chapter

This chapter describes the contents of the guide and contains a disclaimer and a glossary.

About this guide

This document is an informative guide intended to assist product users in achieving a better understanding of cyber security, typical cyber security challenges, and the measures required to protect the reliability, integrity, and availability of variable speed drive systems against unauthorized access or cyber attacks. The aim of the document is to introduce ABB Drives cyber security policies and to help in answering questions and concerns relating to cyber security. The document can be also used as a generic cyber security deployment guide for ABB drives and related connectivity products.

Disclaimer

This document is not intended to be used verbatim, but rather as an informative aid. The examples in this guide are for general use only and do not offer all the necessary details for implementing a secure system.

It is the sole responsibility of the customer to provide and continuously ensure a secure connection between the product and the customer network or any other network. The customer is required to establish and maintain any appropriate measures (including but not limited to the installation of firewalls, application of authentication measures, encryption of data, installation of anti-virus programs, etc.) to protect the product, the network, its system, and the

interface against any kinds of security breach, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB and its affiliates are not liable for damage and/or losses related to such security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

2

Cyber security essentials

Contents of this chapter

This chapter describes the essentials of cyber security, cyber security regulations and standards as well as concept of defense in depth.

Introduction

Traditionally, “cyber security” has been defined to mean all measures taken to protect computer systems and networks against unauthorized access or attack. In the context of power and automation technology, the definition has been redefined to mean measures taken to protect the reliability, integrity and availability of power and automation technologies against attack that may result in unauthorized information disclosure, damage to hardware, software, data, as well as in the disruption of operation.

IT Cyber security covers all the processes and mechanisms by which digital equipment, information and services are protected from unintended or unauthorized access, change or destruction, as well as security measures to ensure the confidentiality, integrity and availability (CIA) of data, both in transit and at rest. In the OT world, the idea is more like preserving the same “CIA” properties but in reversed order: “AIC”. That is because the availability of operation or even safety is considered more crucial than confidentiality compared to the IT world.

Cyber security is of key importance for ABB customers and ABB alike. There are several reasons for that, such as the following:

- Modern automation, protection, and control systems are often highly specialized IT systems leveraging commercial, off-the-shelf IT components and using standardized, IP-based communication protocols.
- The control systems can be also distributed and interconnected, which means an increased attack surface compared to legacy and isolated systems.
- The control systems are extensively based on software.
- DoS (denial-of-service) attacks and malware (e.g., worms and viruses) have become all too common and have already impacted ICS (industrial control systems).
- Computer systems include a very wide variety of smart devices, including smartphones, and networks include not only the Internet and private data networks, but also Bluetooth, Wi-Fi, and other wireless networks.
- Cyber security of industrial control systems typically includes three threat categories:
    - **Hacking**. An attacker specifically targets an industrial control system to, for example, blackmail a site owner or damage the reputation of an automation vendor. This could be achieved by creating dedicated malware. Stuxnet is most likely an example of such a targeted attack.
    - **General malicious software**. Consider a scenario where an employee connects a laptop to the system network or inserts a USB stick into a server. The purpose of these actions could very well be benign, but if the laptop or USB stick is infected with malware, there is a significant risk that the automation system could be infected as well. Even though the malware in these cases hasn't been designed to damage automation systems, it can still be very harmful.
    - **Employee mistakes**. For example, an engineer wants to update the control logic in an embedded device, but by mistake connects the engineering tool to the wrong device, or an engineer connects a network cable to the wrong port of a network switch.
- Most often, hacking is what people think of when discussing cyber security. However, these types of attacks only constitute a minority of all incidents. General malicious software and employee mistakes make up most incidents.

Cyber security in automation applications and networks

Cyber security solutions are reaching almost all automation and operational technology (OT) applications. The concept of the "trusted network" remains useful. The "trusted network" should be understood, from a cyber security viewpoint, as being a strictly limited and well hosted portion of a certain network or control system. So, if it is planned (or even suspected) that some part of a deployment will be in an uncontrolled environment without responsible domain management and physical access control, the system and network should not be regarded as trusted. There, feasible cyber security procedures and policies are always required including adequate countermeasures.

The cyber security approach in automation applications differs from standard business IT applications. Often, it is not possible to upgrade certain control systems, because the operation process cannot be stopped just for software updating. Also, software updates or security patches may be infrequent because each change needs to be tested by vendors in various configurations before patches can be applied in the field.

There are significant risks related to excessively complex requirements or updates for cyber security products and features, which may not guarantee correct operation under all circumstances. So, not all complex IT security tools can be used in automation.

Today fieldbus connectivity is also often a gating requirement for acceptance as a drive's vendor by customers. Because industrial Ethernet protocols have proliferated on the factory floor, there is rising demand to implement hardening features for field-level components too, such as variable speed drives (VSD).

Although fieldbus technologies have been evolving since Modbus (published by Modicon, 1979) almost none of standardized industrial fieldbuses support authentication or any other basic cyber security methods. Only lately standardized protocols have been added with cyber security capabilities. This has been, and still is, the main reason why variable speed drives do not typically offer means to secure network traffic. This is also the reason why drives are seen as vulnerable to malicious system access, data reading and manipulation by hostile parties.

The industrial Ethernet protocol associations have started to migrate to new Ethernet standards that offer higher cyber security protection, but the change will take time.

As stated earlier, often it is not easy to update certain control systems, and all updates need to be carefully verified before patching in the field. On the other hand, the risks are partially mitigated because typically the connectivity to an upper-level automation or controlling (PLC) network requires separate cabling, connections, usage of firewalls and commissioning of the communication interface, e.g., the fieldbus interface of a drive. That is, drives are typically not network-enabled or network-connected by default.

Cyber security and safety

Cyber security in automation aims primarily for retaining a continuous operation. This means that implemented cyber security controls must not compromise the system to perform its essential functions such as operational safety functions. For example, antivirus software must not be permitted to halt the operation of a safety system or process control system under any circumstances.

The same priority applies to remote access solutions. No technological solution may be permitted to hinder a local operator from controlling the operation equipment locally, even if the secure remote access would go to error condition. However, it should be considered that cyber security threats may have consequences on safety related systems and thus compromise safe operation of the control system. Therefore, cyber security threats and vulnerabilities should be considered together with safety hazards to achieve the safest operation capability in the control system.

The first objective in automation is to maintain the safe operation and data even in the following cases:

- Control, support, and backup system malfunction

- Human operator mistakes
- Remote access situations
- Maintenance operations
- Online support
- Malfunctioning device
- Network load increase
- Commissioning

Cyber security regulations and standards in automation

ABB recognizes the importance of cyber security standards, and ABB is an active member of several industry initiatives, including IEEE and IEC. This involvement ensures that the needs of our customers are considered in the development of new standards and that ABB remains abreast of new developments. It also enables ABB as a company to incorporate new standards into ABB's products and systems, helping ABB's customers to comply with regulations as they come into force.

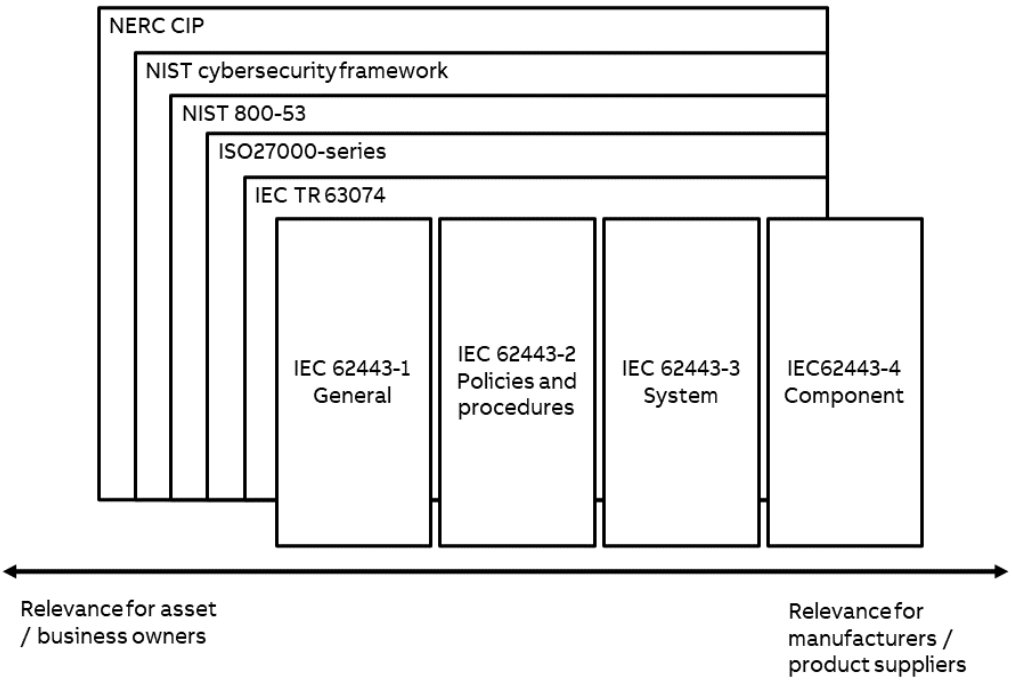
The cyber security regulations in automation affecting ABB are:

- The NIS 2 Directive: The Network and Information Security Directive applies to public and private entities of a type referred to as essential entities and as important entities. The Directive does not apply to entities that qualify as micro and small enterprises within the meaning of Commission Recommendation of European Union.
- The European Cyber Resilience Act: The proposal for a regulation on cyber security requirements for products with digital elements reinforces cyber security requirements to ensure more secure hardware and software products.

In general, the most important cyber security standards in automation are:

- IEC 62443 series: *Industrial communication networks – Network and system security*
- IEC TR 63074: Safety of machinery – Security aspects related to functional safety of safety-related control systems
- NIST 800-53: Security and Privacy Controls for Information Systems and Organizations
- NIST Cyber security Framework: Framework for Improving Critical Infrastructure Cyber security
- NERC CIP: Critical Infrastructure protection standards
- ISO 27000-series: The ISO 27000 series of standards for all information security matters.

The available standards and frameworks are mapped as shown in *Figure 1. Important cyber security standards and frameworks*. They are mapped according to their relevance for asset owners and manufacturers.



There is significant overlap among many of the standards, especially those which are useful for operators or site owners.

The main reference for automation cyber security requirements is documented in standard IEC 62443 (also known as ISA 99) with the widest scope and most detailed guidelines [5]. The NIST Cyber security Framework version 1.0 was published on February 1, 2014 and has less details. Version 1.1 was updated in April 2018 with clarifications and new version 2.0 is under work at the time of publishing this document. NERC CIP is worth mentioning, since at sites that are connected to the bulk electric grid in the US and Canada, it is mandatory to comply with the NERC CIP standard.

The International Electrotechnical Commission (IEC) is a worldwide organization for standardization that continuously develops and maintains all parts of the IEC 62443 series, published under the general title Industrial communication networks – Network and system security. These standards can be purchased from the IEC website. The IEC 62443 series standards with titles are listed in Table 1.

The derivation of cyber security requirements from the aforementioned standards for a specific automation case is not a trivial task. Providing that the necessary safety and operation continuity requirements can be met, the cyber security requirements can be analyzed using the installation environment, use cases and threat landscape as a basis for understanding the cyber security threats.

Table 1. Important cyber security standards and frameworks.

IEC Reference		Title and scope
General	IEC/TS 62443-1-1	*Concepts and models*
	IEC/TR 62443-1-2	Master glossary of terms and abbreviations
	IEC 62443-1-3	Security system conformance metrics
	IEC/TR 62443-1-4	IACS security life cycle and use cases
Policies and procedures	IEC 62443-2-1	Security program requirements for IACS asset owners
	IEC/TR 62443-2-2	IACS Security Protection Ratings
	IEC/TR 62443-2-3	Patch management in IACS environments
	IEC 62443-2-4	Security program requirements for IACS service providers
System	IEC/TR 62443-3-1	Security technologies for IACS
	IEC 62443-3-2	Security risk assessment for system design
	IEC 62443-3-3	System security requirements and security levels
Component	IEC 62443-4-1	Product security development life cycle requirements
	IEC 62443-4-2	Technical security requirements for IACS components

As presented in the above table, IEC 62443 series is organized into four parts presenting security requirements for different levels of industrial automation and control system context. In the next section, the concept of defense in depth is presented which follows similar idea of organizing security measures into different layers. The four different IEC 62443 standard parts also apply differently to different roles related to industrial automation and control systems. These roles are referred in the following section.

Defense in depth

There is no single solution to managing the cyber security risk in an industrial control system, nor is there a completely secure system. Hence, like many other instances, ABB recommends “defense in depth,” which means the coordinated use of multiple security countermeasures and addressing people, technology, and operations in several layers.

Defense in depth is an information assurance concept in which multiple layers of security controls (defenses) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails, or a vulnerability is exploited.

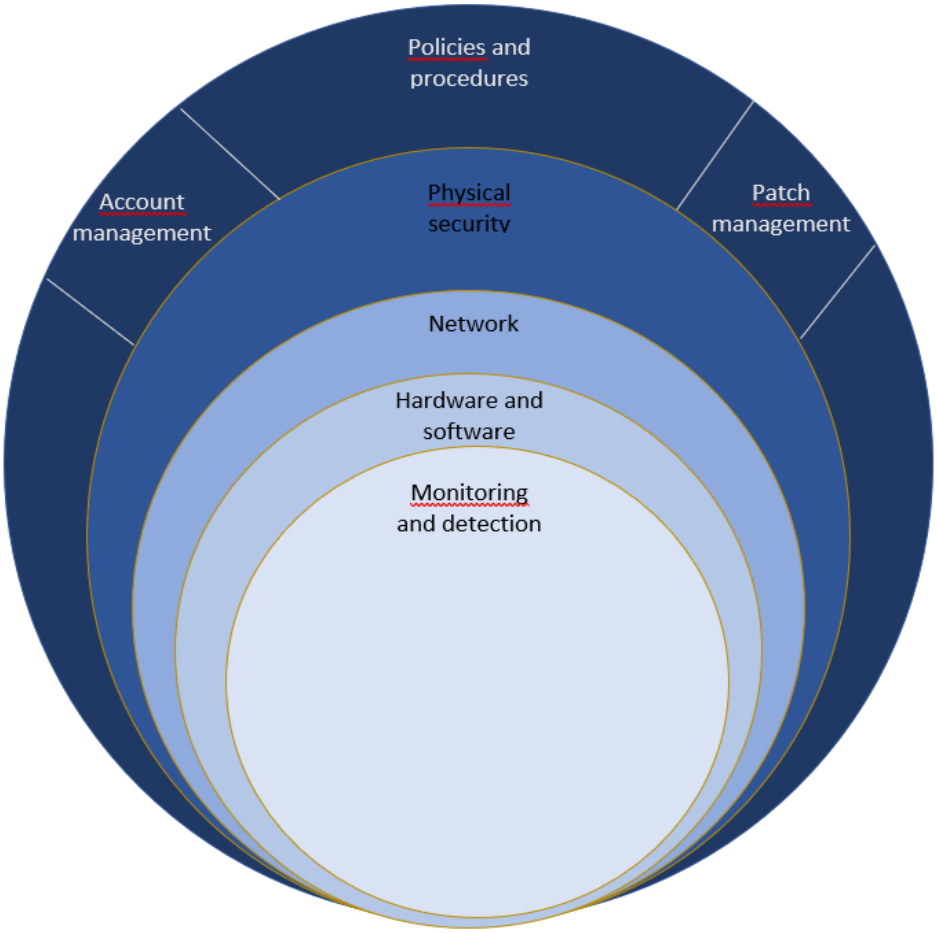


Figure 2. Example of defense-in-depth and multi-layered protections

The idea behind the defense-in-depth approach is to defend a system against any attack using several independent methods. It is a layering tactic, conceived by the US National Security Agency as a comprehensive approach to information and electronic security.

The placement of protection mechanisms, procedures and policies is intended to increase the dependability of an IT system, where multiple layers of defense prevent espionage and direct attacks against critical systems. In terms of computer network defense, defense-in- depth measures should not only prevent security breaches, but also buy an organization time to detect and respond to an attack and so reduce and mitigate the consequences of a breach.

In the IT and OT world, no single defense is impenetrable, and no information security strategy is complete without a defense-in-depth strategy. Implementing this strategy isn't simple for corporations defending their information assets. While castles have the luxury of only one entry point, corporations' business networks have multiple entry points (e.g., support connections with suppliers, service providers and customers), making security more porous. Moreover, there are many more threat vectors now than there were just a few years ago. In the early 1990s, network security was basically a matter of defending against packet-level attacks, and firewalls were glorified routers. Now, internal resources can be compromised through buffer overflows, SQL injection, malicious web pages, malicious active email content, wireless connections, phishing, and more.

It is essential to make sure that controls build depth as opposed to just breadth. The perspective should not be limited to the physical realm, thinking in terms of only physical network and system boundaries. To verify that the defense is genuinely defense in depth, it should be possible to take a given threat and a given asset and find more than one control that protects that asset from the selected risk.

Roles and responsibilities

Usually, the owner of the business has the main responsibility for selecting, deploying, and maintaining the cyber security of applied technical solutions. However, it is practically impossible for one player to control all aspects of cyber security, production continuity and defense in depth layers. Co-operation is needed with many partners to design, construct, and maintain a feasible level of cyber security for continuous operation.

The following list presents examples of actors and their roles ensuring valuable cyber security co-operation. The division of roles is based on IEC 62443 standard series. It should be noted that the same actor can act in several roles. For example, ABB can also have system integration or maintenance responsibilities in addition to product supplier responsibilities.

- **Asset / business owner**. Own and operates industrial automation and control system and provides operational as well as maintenance policies and procedures regarding cyber security.
- **System integrator**. Competence in and experience of valuable cyber security co-operation: platform weaknesses and cyber security bottlenecks in system integration. Validation and approval of all cyber security solutions before their actual commissioning in the field. Adviser on secure usage of devices and applications, upgrades, patches, maintenance, and monitoring services, etc.
- **Maintenance service providers**
    - **Network services**. Maintaining a secure network architecture together with managed switches (VLANs), routers (networks), firewalls (access control), and monitoring services (identification of malicious behavior or software).
    - **Telecommunication network operator**. Establishing and cyber security monitoring of private access points and possibly VPNs for customers.
    - **Office security services**. Physical access control and monitoring of facilities, rooms, cabinets, etc.
- **Product suppliers**
    - **Embedded device providers**. ABB works primarily in this role providing industrial drives and related products.
    - **Software providers**. Maintenance of operation system software, antivirus software, management software, etc.
    - **Network equipment vendor**. Establishing a secure network architecture together with managed switches (VLANs), routers (networks), firewalls (access control).

Defense in depth - generic cyber security policies and controls

Most cyber security risks can be controlled by feasible network architectures, access control and physical security mechanisms. Undisturbed security and management also require a strict cyber security policy and approach that includes various viewpoints and activities to keep up the targeted level of cyber security in automation. The following table presents generic cyber security controls and policies. The table should be read considering the following information:

- The first column presents the defense in depth layers shown in Figure 2. Each layer is identified with unique ID to help referencing across the document.
- The second and third columns present baseline security responsibilities for ABB and its customers. It should be noted that the division of responsibilities is only indicative and does not apply to all product deliveries. Each responsibility is identified with unique ID to help referencing across the document.
- The fourth column presents example security controls.
- The fifth column presents threats addressed by security controls in generic level.

Defense in depth layer (DL)	**ABB**	**Customer (Asset owner / System integrator / Service provider)**	**Example controls**	**Threats addressed**
DL 1 Policies and procedures	DL 1.1 Handling vulnerabilities and security issues	DL 1.1.1 Reporting vulnerabilities and security issues	Web: http://www.abb.com/cyber security Email: cyber security@ch.abb.com Publicly disclosed vulnerability public responses can be found from ICS-CERT - https://ics-cert.us-cert.gov/alerts.	Unnoticed vulnerabilities in systems and products
	DL 1.2 Providing product user documentation on how to securely remove the product from use	DL 1.2.1 Following the recommendations provided	Remove the product from its intended environment.	Exposure of sensitive or confidential information
			Remove references and configuration data stored within the environment.	
			Perform secure removal of data stored in the product. If stored data cannot be removed, perform secure disposal of the product to prevent potential disclosure of data contained in the product.	
	DL 1.3 Providing product user documentation on how to securely operate the product	DL 1.3.1 Following the recommendations provided	Communicate to all users and train them in the established cyber security and change management procedures.	Unintended consequences caused by trusted actors
	DL 1.4 Providing product user documentation on how to harden the product	DL 1.4.1 Following the recommendations provided	Disable the SSH service (factory support account) when SSH console for support and diagnostics is not needed.	Enlarged attack surfaces
			Use HTTPS instead of HTTP where applicable.	
			Disable NTP (Network Time Protocol) requests that IoT gateway can send to external servers or replace with local NTP time servers if such are available.	

DL 2 Account management	DL 2.1 Providing product user documentation on requirements and recommendations on how to manage the user accounts associated with the product	DL 2.1.1 Following the recommendations provided	Create only those accounts that will be used locally or remotely, using roles with as few access rights as possible. Use strong passwords.	Enlarged attack surfaces Unauthorized access to system
			Remove default accounts.	
			If ABB cloud services are used (for example, ABB Ability™ Digital Powertrain - Condition Monitoring for drives): Regularly verify the given e-mail accesses for the CIAM accounts to avoid misuse, and communicate wrong or expired accounts immediately to ABB.	
			Change the default administrator password in products where they are used.	
DL 3 Patch management	DL 3.1 Providing security updates in a timely manner	DL 3.1.1 Installing the provided security updates accordingly	Install trusted signed SW packages only from trusted sources (e.g., from ABB Drives site with HTTPS).	Malware Remote code execution
			Check that the latest firmware version of the IoT gateway is being used to have the latest software versions and security patches in use.	
DL 4 Physical controls	DL 4.1 Providing product user documentation about the measures expected from the environment	DL 4.1.1 Following the recommendations provided	Tamper detection of unauthorized access (for example, inspecting sealing)	Injection of malicious code through physical interfaces Device breakage Eavesdropping and tampering of network traffic
			Tamper-resistant equipment (for example, disabling debug interfaces)	
			Locking of facilities and rooms	
			Locking devices for the cabinets	
			Physical access based on work permits, asset security and CCTV monitoring (video surveillance)	

DL 5 Network controls	DL 5.1 Providing product user documentation about the measures expected from the environment	DL 5.1.1 Following the recommendations provided. For example, recommended configuration of firewall and network segmenting measures	Use HTTPS for tool communication. Unsecure protocols may be used only when they are properly justified based on risks.	Eavesdropping / tampering of data in transit.
			Connect each building automation firewall with the control room firewall using static secure VPN gateway-to-gateway connections.	Eavesdropping / tampering of data in transit.
			Deny all connections from/to the building automation networks and other networks	Unintended traffic, Loss of availability, Denial of service Access by unauthorized actors
			Deploy and securely manage the firewalls in the front of each building automation network	Ineffective or compromised firewall
			Ensure all non-used connections are deactivated	Unintended traffic, Loss of availability, Denial of service Access by unauthorized actors
DL 6 Hardware and software controls	DL 6.1 Implementing cyber security features and capabilities according to product's cyber security requirements and industry best practices	DL 6.1.1 Ensuring that the cyber security functionality is enabled and correctly configured (see Policies and Procedures: Hardening)	Set a master password to prevent eg., the changing of parameter values and/or the loading of firmware and other files	Unreached target security level
			Input validation	
			Encrypting data at rest and in transit using secure protocols such as TLS with secure cryptographic ciphers and parameters	
			Use endpoint protection with appropriate maintenance	
			Change the default administrator password.	
DL 7	DL 7.1 Providing instructions and recommendations	DL 7.1.1 Establish network cyber security	Actively monitor the internal network. Specifically track for any unauthorized devices. Monitor the system logs for	Unauthorized devices

Monitoring and detection	for the use of monitoring and detection systems relevant to the product.	monitoring systems and ensure that these cannot negatively affect the system operation under any circumstances.	unauthorized access or other suspect behavior.	connecting to trusted networks Undiscovered devices
			Monitor the cyber security, topology (asset management) and correct operation of the plant networks using the cyber security monitoring modules and features of the firewalls and managed switches	

Generic cyber security solutions in product life cycle

Automation system operation can fail totally due to the reason that cyber security was not put in place and protection features were not used.
Secure operation must be tested in all possible use cases of an automation system. Penetration testing can reveal the hidden threats in the overall system, so such an opportunity should be arranged at the integration site before letting the automation system setup go to the production phase. In penetration testing, external experts that are familiar with e.g., hacking tools and methods may be needed.

Cyber security levels and their accompanying requirements help to understand whether cyber security is covered sufficiently in a project or in an operational automation service. Good examples of cyber security requirements and levels can be found in IEC 62443-3-3, *System Security Requirements and Security Levels* [7] (see section *Cyber security regulations and standards in automation*). Requirements should be applied according to identified threats.

The targeted cyber security level can be maintained by constantly monitoring the new vulnerabilities in products that are used and applying the related software patches whenever possible. Networks need to be monitored against unauthorized access and spy software. It is not possible to act without knowing what threats can be encountered every day. It is important to track who is present in a network and if someone is trying to access it without permission, for example through a firewall protection layer. There are also network cyber security monitoring services available that can be used and guided specifically to report any anomalies or attacks that occur during the operation of an automation system.

Cyber security must be considered in all phases. The table below lists typical cyber security considerations in different project phases. The activities are partially the same as in the table presented in section *Defense in depth - generic cyber security policies and controls*. The activities are also referenced with corresponding IDs.

Phase	Cyber security activity
Deployment & pilot phases	Install the firewalls and remote access (VPN) solution according to company policy and cyber security requirements. DL 1.4.1, DL 5.1.1, DL 6.1.1
	Enable remote access only for authorized vendor personnel with authorized user accounts. DL 2.1.1
	Restrict (each user account) access from different vendors to subnetworks or machines belonging to the delivery. DL 2.1.1
	Install trusted signed SW packages only from trusted sources (e.g., from ABB Drives site with HTTPS). DL 3.1.1
	Install vendor-approved patches. DL 3.1.1
Commissioning phase	Hardening of systems. Check and ensure that there is a specific cyber security configuration in all network and automation devices, systems, and software according to the deployment guidelines. All unnecessary software and features should be removed from the delivery. DL 1.4.1, DL 5.1.1, DL 6.1.1
	Test that all systems and cyber security mechanisms work according to the specifications.
	Communicate to all users and train them in the established cyber security and change management procedures. DL 1.3.1
	Establish network cyber security monitoring systems and ensure that these cannot negatively affect the system operation under any circumstances. See DL 7.1.1.
Maintenance	Keep up the hardening by strict access and change control, allowing only planned changes and patches to systems including ABB products, network devices and operating systems. DL 1.4.1, DL 5.1.1, DL 6.1.1
	Monitor the system logs for unauthorized access or other suspect behavior. DL 7.1.1
	Plan and test system upgrades and new features in test facilities before applying them to production systems. DL 3.1.1
Decommissioning	Remove the product from its intended environment. DL 1.2.1
	Remove references and configuration data stored within the environment. DL 1.2.1
	Perform secure removal of data stored (for example parameters and settings) in the product. DL 1.2.1
	If stored data cannot be removed, perform secure disposal of the product to prevent potential disclosure of data contained in the product. DL 1.2.1
	Reset the product to factory default configuration

Visualized defense in depth layers

The following figure presents a simplified security architecture. The defense in depth layers presented in this document are visualized as colored labels and related example controls are labeled with matching colors in the diagram. Every control is then referenced with a corresponding ID from the table in section *Defense in depth - generic cyber security policies and controls*.

The table also presents a rough division of security responsibilities between ABB and customer where ABB Motion works as a product supplier and is only responsible to secure the delivered product and giving recommendations and guidelines for customers related to their security responsibilities. However, it should be noted that there are customer cases where ABB works also in a different role for example, as a system integrator where the division presented below is different.

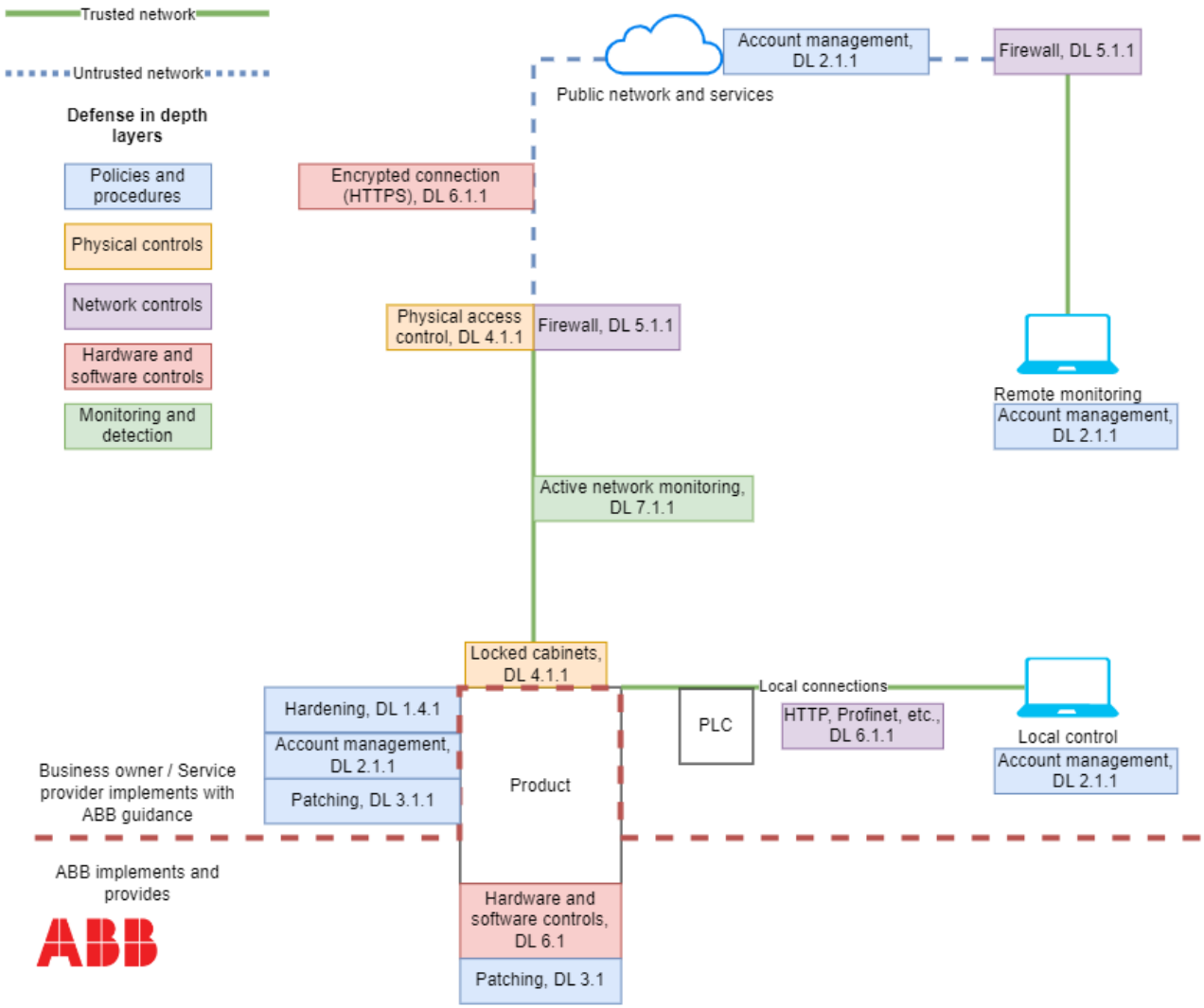


Figure 3. Defense in depth layers.

3

Example cases

Contents of this chapter

The next few sections describe four different application environments where ABB variable speed drives and connectivity products are typically used. For each case, we introduce typical use cases, challenges from the cyber security point of view and secure deployment practices – that is, generic resolution and mitigation of identified cyber security challenges and risks.

Introduction

The goal of “secure by deployment” is to ensure that products can be installed, configured, operated, and maintained in a secure way. This includes deployed software remaining free from known vulnerabilities or security weaknesses.

As is shown in each case, ABB Drives products enable remote networked operation and monitoring. These networking and connectivity capabilities increase the importance of hindering all unauthorized electronic access to automation systems.

Case 1 – Industrial automation example (factory environment)

Description

This example describes generic means of protecting the industrial automation environment against unauthorized access.

Industrial automation systems vary a lot in practice. There are many different networks and automation application architectures implemented globally within different industrial sectors, such as manufacturing, process industry, power generation and distribution. That is why this example is for general use only and does not offer all the necessary details for implementing a secure system. But all the guidelines and instructions for deploying ABB drive and connectivity products are real and valid.

The concept of defense in depth should be applied also regarding physical security protection. Example generic physical security measures consist of the following:

- restricting access to factory/plant area
- restricting access to the rooms where devices are located
- restricting access to device cabinets
- restricting access to the device management or physical ports
- detection and notification of physical tampering

Figure 4 depicts a fictitious plant network utilizing ABB Drives products that is usually connected securely to the customer's corporate networks (not visible in the image) via public or private networks, but also to other automation field networks within the plant.

In this example, industrial drives (e.g., ACS880), are used to represent variable speed drives. The other generic examples of ABB Drives connectivity and software products shown are:

- Safety PLC (programmable logic controller e.g., AC500 / AC500-S)
- Ethernet communication for drives using Ethernet adapter modules (FPNO-21, FEIP-21, FMBT-21) or an integrated solution
    - Currently cyber security features of industrial Ethernet protocols (Modbus/TCP, Ethernet/IP and PROFINET IO) are not supported
- IoT gateway (e.g., NETA-21). Remote monitoring for drives
    - Implements security features for communicating over untrusted networks
    - Includes user authentication, user accounts, and secure communication.
- Integrated software suite for machine builders and system integrators to automate their machines and systems (e.g., Automation Builder with Drive Manager plug-in)
    - Combines the tools required for configuring, programming, debugging and maintaining automation projects from a common interface
- Software tool for start-up and maintenance of ABB's common architecture drives (e.g., Drive Composer)
    - Used to view and set drive parameters, and to monitor and tune process performance.

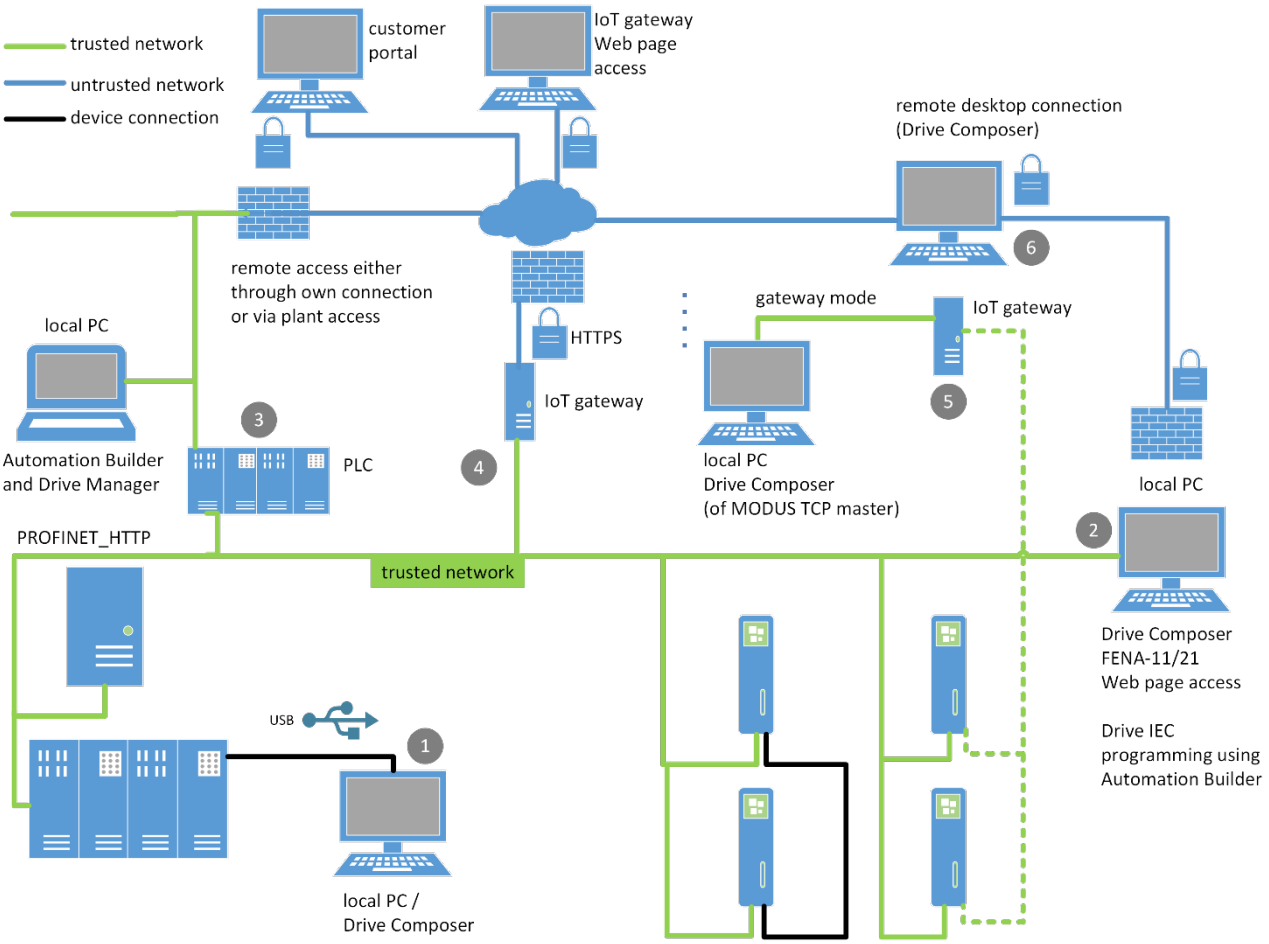


Figure 4. Industrial automation plant. Different network possibilities and their secure deployment.

Figure 4 shows several different use cases and communication possibilities. See the figure for the numbers referred to below. The shown use cases are:

- **Commissioning** of the drives and production line using the start-up and maintenance tool and/or integration suite tool via:
  - local connections (point-to-point serial communication, i.e., USB), or
  - shared (with control) upper-level physical fieldbus network (e.g., PROFINET) using Ethernet tool communication, and/or
  - communicating also through the PLC system using a plug-in device tool (e.g., Drive Manager), or
  - IoT gateway remote monitoring tool web interface, or
  - IoT gateway acting as a gateway between, or
  - a third-party remote desktop connection.
- **Maintenance and troubleshooting** using the above-mentioned tools and communication networks

Remote support and remote condition monitoring services

- **On-demand based remote monitoring** over untrusted network (public Internet) using the IoT gateway remote monitoring tool.

The architecture illustrated includes the following components:

- In public networks, there are services such as:
  - Customer Portal (cloud service)
  - Remote monitoring via Web page access, e.g., IoT gateway
  - Remote desktop connections (start-up and maintenance tool)
- In the trusted plant network, there are:
  - Firewalls in front of public networks
  - PLCs and local PCs (different software tools installed)
  - Drives that are connected to Ethernet fieldbus (e.g., PROFINET) via ethernet adapter module or via integrated solution
  - Drives that are connected to a local PC via USB
  - IoT gateway, that is also connected to public networks via firewall
  - IoT gateway that is connected to the drives with EIA-485 and to a local PC using gateway mode.

Cyber security risk mitigation and secure deployment

The idea is to create defense-in-depth protection for each network by allocating firewall solutions to the front of internal trusted networks of each network

- Carefully manage firewalls, their configurations and access rules.

Ethernet fieldbus adapters deployment

Ethernet adapter module must be positioned in a trusted network (strictly limited and well hosted portion of a network or control system)
On the ethernet adapter module service configuration page (web page) certain Ethernet services can be disabled. All services are enabled by default. It is recommended to disable services that are not used after commissioning:

- PC tool communication or access to ethernet adapter module web pages
- Change of IP settings remotely using ABB IP configuration tool
- Remote access to drives with start-up and maintenance tool via Ethernet tool network
- Ping response.

For more information, see the different fieldbus manuals available in the list of references.

Industrial drives deployment

User lock. For better cyber security, it is possible to set a master password to prevent e.g., the changing of parameter values and/or the loading of firmware and other files. The user lock feature makes it possible to prevent:

- firmware upgrades[1]
- safety functions module (e.g., FSO-12/-21) configuration
- parameter restoration
- loading of adaptive or application programs
- changing home view of control panel
- editing drive texts
- editing the favorite parameters list on the control panel

[1] Firmware integrity can be verified by using SHA checksum from released upgrade package from sales release note of corresponding firmware release from ABB library (or other trusted source)

- configuration settings available through control panel such as time/date formats and enabling/disabling clock display.

User access levels

Configure for local user interfaces (start-up and maintenance tool and control panels) parameter access rights using parameter lock feature.
For more information, see the different drives primary control program manuals available in the list of references.

Start-up and maintenance PC tool Ethernet tool communication deployment

Start-up and maintenance tool establishes Ethernet communication only with “recognized devices”, that is, ethernet fieldbus adapters. This is the default mode of operation.
For more information, see *Ethernet tool network for ACS880 drives application guide* [17].

IoT gateway deployment

Configure the cyber security features of IoT gateway according to the principle of denying everything that is not needed nor used.

- Change the default administrator password.
- Create only those accounts that will be used locally or remotely, using roles with as few access rights as possible. Use strong passwords.
- Check that the latest firmware version of the IoT gateway is being used to have the latest software versions and security patches in use.
- If ABB cloud services are used (for example, ABB Ability™ Digital Powertrain - Condition Monitoring & Remote Assistance): Regularly verify the given e-mail accesses for the myABB accounts to avoid misuse, and communicate wrong or expired accounts immediately to ABB.

For secure access, use HTTPS, which is a combination of HTTP with an added encryption layer of SSL/TLS protocols to create a secure channel over an insecure network.
If the highest possible degree of product hardening is required, then it is possible to also do the following modifications:

- Tool settings (factory tools): check the SSH service (factory support account) is disabled when SSH console for support and diagnostics is not needed.
- Locale settings: set local NTP (Network Time Protocol) server instead of using external ones.
- Device interfaces / Ethernet (interface settings): disable the background scan that broadcasts UDP discovery requests on the local network to discover Ethernet-connected ABB drives.

The following network services should be disabled if they are not used:

- NBT NS discovery (NetBIOS name discovery service)
- FTPS service, even though no FTP(S) accounts exist by default
- Ethernet tool network, automatic discoverability of IoT gateway within local network.

If an IoT gateway and a start-up and maintenance tool are used at the same time over Ethernet, the PC tool-friendly mode should be used in IoT gateway.
Actively monitor the internal network. Specifically track for any unauthorized devices.
For more information, see the different IoT gateway manuals in the list of references.
Customer portal and cloud related security aspects are described in *Security Overview - Drive Remote Service Platform* [9] (available in ABB Library).
Cloud services require only an out-bound HTTPS (port TCP:443) connection from IoT gateway to servers in Microsoft Azure. Cloud services use central user authorization and management such as ADFS (Active Directory Federation Services).

Normal hardening instructions for IoT gateway apply also in the context of cloud services. It is also possible to close the entire web interface of IoT gateway over the cloud connection (for example, if IoT gateway is connected to a public network).

Case 2 – Remote pumping stations

Description

This example describes generic means to monitor, operate and maintain remote pump stations (booster pump application) in real time using permanent wireless connections. In addition to an industrial automation plant example, it also illustrates the possibility that drives can be connected to the Drivetune mobile app via a Bluetooth interface (ACS-AP- W) and the mobile app operating as a gateway can connect drives to the Internet via mobile (3G/4G) networks. In this example, ABB's ACS580 general purpose drives are used to represent variable speed drives.

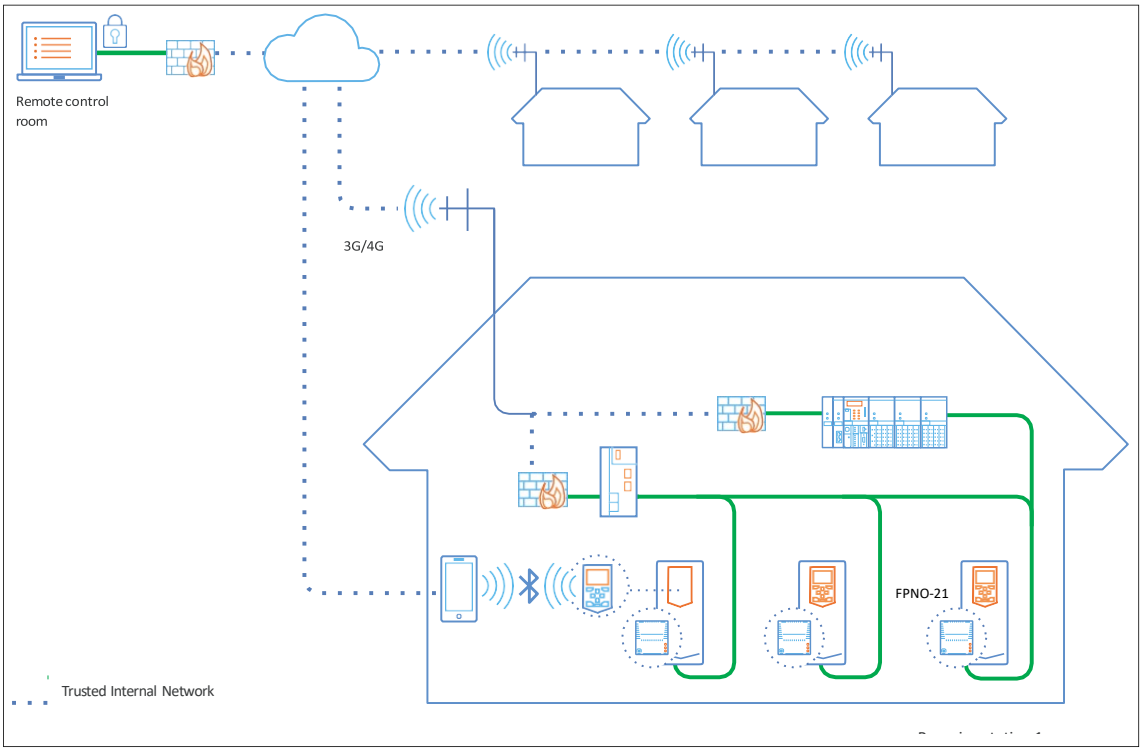


Figure 5. Water Pumping Station with permanent wireless connections.

In this example, solution drives can control one or several pumps and thus the water volume flow based on need. The new technology and control methods make it possible to save significant amounts of energy, but from the cyber security point of view, this approach increases the number of field automation devices and cyber security-related risks. Remote connections have been implemented typically for local PLC or SCADA systems.

The challenge is how to secure the station networks and the connections.

- A distributed architecture increases the need to restrict access to other local stations and operator systems.
- Loose physical access control means that the local network cannot be stated as trusted and implies that defense in depth must be implemented.

Cyber security risk mitigation and secure deployment

The idea is to create defense-in-depth protection for the pumping station as follows:

- Allocate a dedicated cellular operator access point (APN) for all wireless connections with pump stations. Each allocated wireless router should only establish and accept connections via a trusted cellular operator access point with customer-agreed cyber security features. (APN is the name of a gateway between a GSM, GPRS, 3G or 4G mobile network and other networks).
- Allocate firewall solutions to the front of the internal (trusted) networks of each pump station: Carefully manage all firewalls, their configurations and access rules.

General purpose drive deployment:

See section *Cyber security risk mitigation and secure deployment* on page 28 for deployment instructions. Follow the same procedures. [11]

Ethernet fieldbus adapter deployment:

See section *Cyber security risk mitigation and secure deployment* on page 28 for deployment instructions. Follow the same procedures. [14]

Start-up and maintenance PC tool Ethernet tool communication deployment:

See section *Cyber security risk mitigation and secure deployment* on page 28 for deployment instructions. Follow the same procedures. [17]

Mobile app for wireless access, assistant control panel and Bluetooth connection deployment:

- Disable the Bluetooth connection when it is not needed. At the very minimum, disable at least the *always discoverable* mode that keeps the ACS-AP-W assistant control panel discoverable to any Bluetooth device within wireless range.
- If the always discoverable mode is needed, make sure the PIN code used for pairing process is kept in a secure place and only authorized persons have access to it.

IoT gateway deployment:

Configure the cyber security features of the IoT gateway in the same way as in the first case. See section *Cyber security risk mitigation and secure deployment* on page 28 for more detailed deployment instructions for the IoT gateway.

Case 3 – Machinery OEM Equipment

Description

This example case is like the industrial automation case, the difference and specific addition being the OEM vendor's remote service connection. OEM manufacturers are often willing to monitor and offer remote support for their machinery and for ABB variable speed drives inside that machinery. This remote connection is typically implemented via a third-party VPN connection (including hardware devices and software). In this example, ABB's ACS380 and ACS880-M04 machinery drives are used to represent variable speed drives.

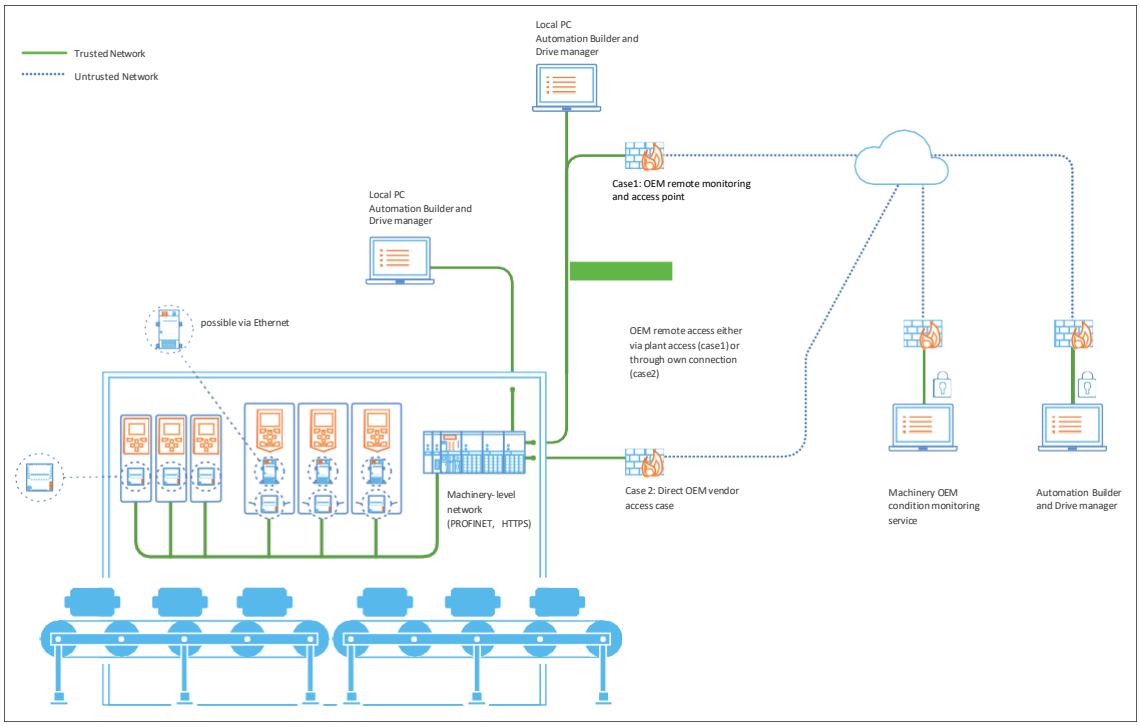


Figure 6. Machinery OEM case.

In this example, the OEM machine (a bottling machine) is a standalone machine or part of a factory automation network including several variable speed drives, PLCs, and other required accessories.

The OEM has two options for the remote connection to the machinery at the end customer's plant:

- Via the customer's networks, firewalls, and access points
- Directly from the OEM machine through a modem, VPN router or similar (not recommended).

The OEM vendor provides a service to keep the machine in operation by managing and installing the OEM machine system, software, and settings remotely. Services can include condition monitoring, optimization, remote support, and software updates.

The end user sees the OEM machine as one system, even if it may also contain PLC and internal field network and other controlling units. End users control the overall machine operation using HMI or via plant level network.

Cyber security risk mitigation and secure deployment

The idea is to secure a remote access path for OEM vendor-specific services.

Case 1: OEM access via the customer's network, firewalls, and access point:

- Deploy and securely manage the firewalls in the front of the plant-level network.
- Connect the corporate firewall to the OEM vendor firewall using static secure VPN gateway-to-gateway connections.
- Deny by default all connections from the machinery networks to other networks.
- Allow only authenticated and secured (HTTPS) service connections between OEM machinery and OEM machinery remote tools.
- Deploy the dedicated managed switch(es) for the use of plant-level networks.
- Separate the different field networks into different segments and deny all unnecessary data communication between the segments.

- Learn and use the cyber security features of the managed switch so that all unnecessary activity is blocked in the subnetworks.
- Separate the management systems and connections to separate network segments with all necessary cyber security features on.
- Deny all other connectivity mechanisms from the machine-level systems to restrict unauthorized access as much as possible.
- Monitor the cyber security, topology (asset management) and correct operation of the plant networks using the cyber security monitoring modules and features of the firewalls and managed switches.

Case 2: Direct OEM vendor access case (not recommended)

- Allocate a dedicated cellular operator access point (APN) for a machine OEM vendor to access.
- The allocated wireless router should only establish and accept connections via a trusted cellular operator access point with customer-agreed cyber security features.
- Allocate firewall solutions to the front of the OEM machine. Carefully manage the firewall, its configuration and access rules.
- Carefully disable all unused services from all components to reduce the attack surface.
- Actively monitor the internal network nodes and behavior of machines using cyber security monitoring services. Specifically track for any misconfigured devices and possible malware behavior patterns.

In both cases, the deployment of ABB drive and connectivity products follows the principles shown in the industrial plant example.

Machinery drive deployment:

See section *Cyber security risk mitigation and secure deployment* on page 28 for deployment instructions. Follow the same procedures. [12]

Ethernet fieldbus adapters deployment:

See section *Cyber security risk mitigation and secure deployment* on page 28 for deployment instructions. Follow the same procedures. [14]

Start-up and maintenance PC tool's Ethernet tool communication deployment:

See section *Cyber security risk mitigation and secure deployment* on page *28* for deployment instructions. Follow the same procedures. [16], [17]

Case 4 – Building automation

Description

This example describes generic means for remote monitoring of geographically distributed buildings and has similarities with the remote pumping station example. The main purpose is to monitor, control and update in real time several buildings and building systems from a control room. In this example case, ABB's ACH550 and ACH580 HVAC (heating, ventilation, and air conditioning) segment-specific drives are used to represent variable speed drives in general.

The other related ABB Drives connectivity products together with ACH550 and ACH580 drives shown are:

- A BACnet/IP adapter module (e.g., FBIP-21) is an optional device for ABB drives, e.g., the ACH580, enabling the connection of the drive to a BACnet/IP network.
- A BACnet/IP router module is (e.g., RBIP-01) is a BACnet router. It is a snap-on module, fitted inside the drive and fully compatible with all ABB ACH550 standard drives for HVAC.

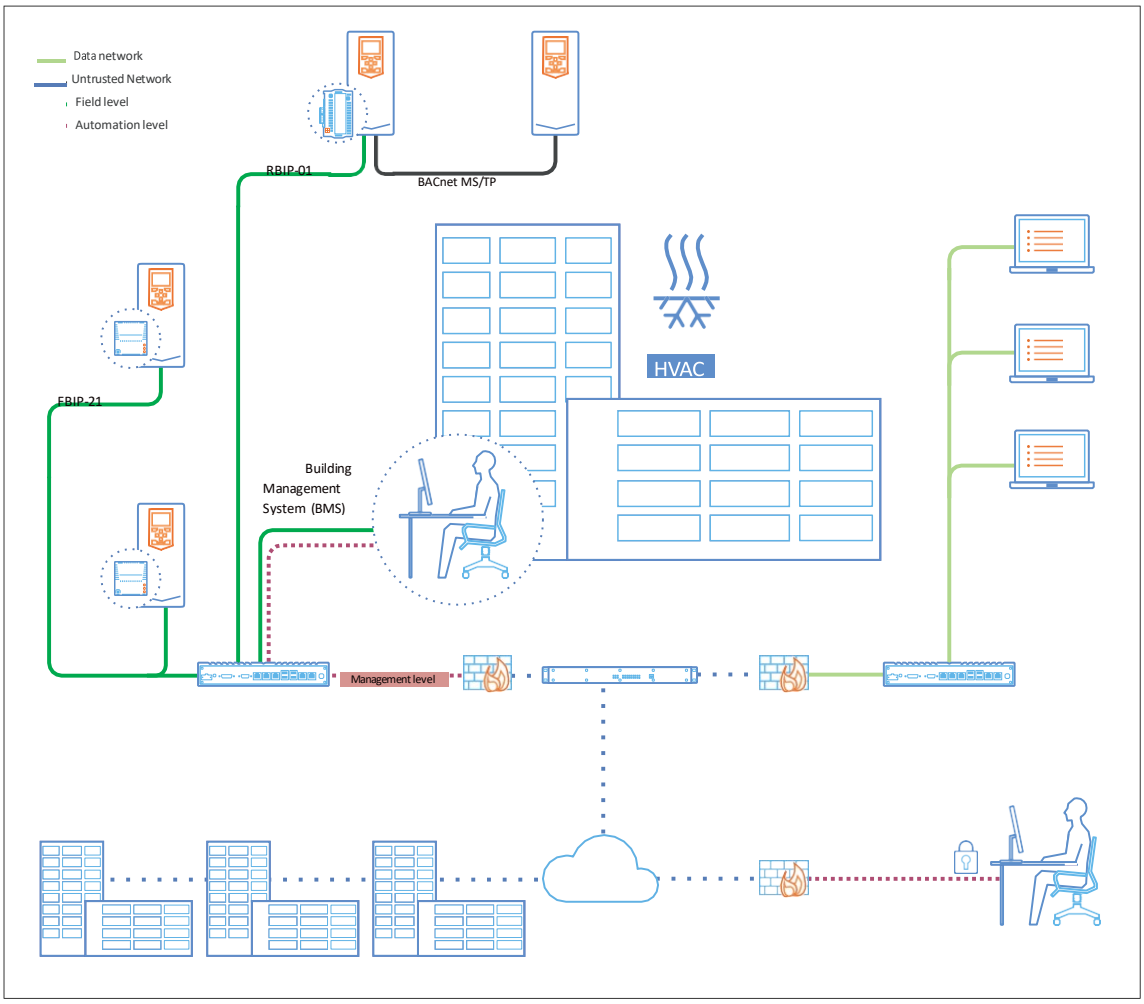


Figure 7. Building automation case.

In this example, there is a need for secure remote connections to several buildings around the city (only campus areas and such may have their own local control room). The data via the remote connections typically comprise:

- alarms and other events
- weekly scheduling (not monitoring for individual devices)
- gathering of different consumption information to the central server.

Typically, there is the utilized building's own BMS (building management system) controller, which runs scheduled timings and control loops, and generates logs. Often, all devices share the same physical and logical LAN for operation and management, also between buildings:

- all automation in the same network (automation level)
- separated LAN for the data of users in buildings (data network)separation can be realized physically or virtually using switches but may share the same Internet connectivity and firewalls.
- The challenge is how to secure the building networks and the connections:
- lots of cabling everywhere, also wireless devices installed
- difficult to control physical access to cabling everywhere

- shared IP network both for operation and management purposes.

Cyber security risk mitigation and secure deployment

The idea is to separate and segment the different local building networks:

- Deploy and securely manage the firewalls in the front of each building automation network.
- Connect each building automation firewall with the control room firewall using static secure VPN gateway-to-gateway connections.
- Deny all connections from/to the building automation networks and other networks.
- Allow only authenticated and secured (HTTPS) management connections between the BMS and control room.
- For securing file transfer, enable SFTP (SSH file transfer protocol).
- Deploy dedicated managed switch(es) for the use of building automation networks.
- Separate the different building automation networks into different segments and deny all unnecessary data communication between the segments.
- Learn and use the cyber security features of the managed switch so that all unnecessary activities are blocked in the subnetworks.
- Separate the management systems and connections to separate network segments with all the necessary cyber security features on.
- Deny all other connectivity mechanisms from the building automation systems to restrict unauthorized access as much as possible.
- Monitor the cyber security, topology (asset management) and correct operation of the building data networks using the cyber security monitoring modules and features of the firewalls and managed switches.

In this example, the deployment of ABB drive and connectivity products follows the principles shown in the industrial plant example.

HVAC drive deployment:

See section *Cyber security risk mitigation and secure deployment* on page 28 for deployment instructions for ACS880. Follow the same procedures. [13]

4

ABB cyber security policies

Contents of this chapter

This chapter describes the ABB policies related to cyber security.

Principle

ABB takes all cyber security-related concerns seriously and has been relentlessly following programs aimed at developing and improving product features and processes, which, in close co-operation with ABB's vendors and customers, help in selecting, deploying, and maintaining the cyber security of applied technical solutions without substantially sacrificing functional safety or operational performance or productivity.

ABB products are aimed at reducing business risk, providing comfort and confidence, as well as enabling compliance with standards and legal requirements. ABB also emphasizes that the cyber security is not a destination, but an evolving target requiring well-established processes to be in place.

ABB is committed to providing its customers with products, systems and services that clearly address cyber security. Proper and timely handling of cyber security incidents and software vulnerabilities is one important factor in helping customers minimize risks associated with cyber security. ABB has therefore established a formal vulnerability handling policy which will be applied at least in the following events:

- An external party (e.g. customer, researcher, government organization) approaching ABB reporting a potential vulnerability affecting an ABB product
- A vulnerability disclosed publicly affecting an ABB product
- A vulnerability being discovered internally that impacts the installed base
- Malware targeting ABB products

Suppliers for ABB have a crucial role in the cyber security program. It is therefore expected that suppliers support and complement ABB's efforts to keep the systems secure. The ABB Cyber Security Requirements for Suppliers establish the minimum measures that we expect our suppliers to comply with. The measures shall be fulfilled for any software-related product that is supplied to ABB.

Device Security Assurance Center (DSAC)

ABB has defined cyber security requirements for all ABB products. The requirements are applicable to any ABB product or system that is software related. ABB strives to continuously improve the security and robustness of its products, and integrated security testing is part of the development process. A dedicated, independent security test center has been established where ABB products are subject to security and robustness tests. The objective of the Device Security Assurance Center is to provide continuous protocol- stack robustness and vulnerability assessments of embedded devices, including four basic categories of tests:

- Basic hygiene testing to check on least privilege principle and performing vulnerability assessment
- Mobile application testing for identifying vulnerabilities in the mobile application
- Communication robustness testing to check on how communication stack can withstand anomaly traffic (flooding and fuzzing)
- Web Application and API testing to check on vulnerabilities in web application and whether there is any security flaw in APIs

A suite of state-of-the-art open source and commercial solutions are used for testing.

Appendices

Glossary

Terms and abbreviations used in this guide.

Term or abbreviation	Explanation
2G, 3G, 4G, 5G	The second, third, fourth and fifth generations of mobile telecommunications technology
Access control	Protection of system resources against unauthorized access
ADFS	Active Directory Federation Services
APN	Access point name is the name of a gateway between a GSM, GPRS, 3G, 4G or 5G mobile network and other networks
Authenticate	Verify the identity of a user, user device or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission
Authentication	Security measure designed to establish the validity of a transmission, message or originator or a means of verifying an individual's authorization to receive specific categories of information
Authorization	Right or permission that is granted to a system entity to access a system resource
Availability	Ability of an item to be in a state to perform a required function under given conditions at a given instant or over a given time interval, assuming that the required external resources are provided
BACnet BACnet/IP	BACnet is a communications protocol for building automation and control networks. Defines the MS/TP (master-slave/token-passing) network. BACnet/IP has been developed to allow the BACnet protocol to use TCP/IP networks
BMS	Building management system
CIAM	Customer and identity access management
CCTV	Closed-circuit television, also known as video surveillance
Change management	Process of controlling and documenting any change in a system to maintain the proper operation of the equipment under control
Compromise	Unauthorized disclosure, modification, substitution, or use of information
Confidentiality	Assurance that information is not disclosed to unauthorized individuals, processes, or devices
Denial of Service (DoS)	Prevention or interruption of authorized access to a system resource or the delaying of system operations and functions or loss of operation
FTP	File transfer protocol

FTP(S)	SSH file transfer protocol, or secure file transfer protocol, is a network protocol that provides file access, file transfer and file management over any reliable data stream
Firewall	A network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules
GPRS	General packet radio service is a packet-oriented mobile data service on the 2G and 3G cellular communication system's global system for mobile communications (GSM)
GSM	Global system for mobile communications, the 2nd generation (2G) of mobile telecommunications technology
Hardening	The process of securing a system by reducing its surface of vulnerability
HMI	Human–machine interface
HTTP	Hypertext transfer protocol is an application protocol for distributed, collaborative, hypermedia information systems
HTTPS	Also called HTTP over TLS, HTTP over SSL, and HTTP Secure, is a protocol for secure communication over a computer network that is widely used on the Internet
IACS	Industrial automation and control systems
ICS	Industrial control system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
Incident	Event that is not part of the expected operation of a system or service that causes or may cause, an interruption to, or a reduction in, the quality of the service provided by the system
Integrity	Quality of a system reflecting the logical correctness and reliability of the operating system, the logical completeness of the hardware and software implementing the protection mechanisms, and the consistency of the data structures and occurrence of the stored data
IP (Internet Protocol)	Network layer communications protocol in the Internet protocol suite for relaying datagrams across network boundaries
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information technology. Computer-related assets of an organization that represent nonphysical assets, such as software applications, process programs and personnel files
LAN	Local area network
NERC	North American Electric Reliability Corporation

NIST	National Institute of Standards and Technology
NBT NS	NBT NS is a daemon for the NetBIOS name discovery. Allows finding computers from a local network by using the NetBIOS host name
NTP	Network time protocol is a protocol for synchronizing computer clocks over a network.
OEM	Original equipment manufacturer is a term used when one company makes a part or subsystem that is used in another company's end product
OT	Operational technology. Hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events
Patch management	Area of systems management that involves acquiring, testing, and installing multiple patches (code changes) to an administered computer system
PLC	Programmable logic controller. Programmable microprocessor-based device that is used in industry to control assembly lines and machinery
PROFINET	Open standard for industrial Ethernet
SCADA	Supervisory control and data acquisition
SSH	Secure shell is a cryptographic (encrypted) network protocol to allow remote login and other network services to operate securely over an unsecured network
SSL	Secure sockets layer. See *TLS*.
TLS	Transport Layer Security and its predecessor SSL are cryptographic protocols designed to provide communications security over a computer network (privacy and data integrity between two communicating computer applications)
TR	Technical report of IEC
TS	Technical specification of IEC
USB	Universal serial bus
VLAN	Virtual local area network. Any broadcast domain that is partitioned and isolated in a computer network at the data link layer

List of references

General guides		Code (English)
[1]	*The NIS 2 Directive* *https://www.nis-2-directive.com/*	
[2]	*Cyber Resilience Act* *https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act*	
[3]	*IEC 62443 series standards, Industrial communication networks – Network and system security* *https://www.iec.ch/blog/understanding-iec-62443*	
[4]	*IEC TR 63074, Safety of machinery – Security aspects related to functional safety-related control systems* *https://webstore.iec.ch/publication/31572*	
[5]	*ISO 27000-series: The ISO 27000 series of standards for all information security matters.* *https://www.iso.org/isoiec-27001-information-security.html*	
[6]	*NERC CIP: Critical Infrastructure protection standards* *https://www.nerc.com/pa/Stand/Reliability%20Standards%20Complete%20Set/RSCompleteSet.pdf*	
[7]	*NIST Cyber security Framework: Framework for Improving Critical Infrastructure Cyber security* *https://www.nist.gov/cyberframework*	
[8]	*Security and Privacy Controls for Information Systems and Organizations* *https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final*	
[9]	*Security Overview – Drive Remote Service Platform*	*9AKK106930A8297*
[10]	*The ABB Cyber Security Requirements for Suppliers* *https://search.abb.com/library/Download.aspx?DocumentID=9AKK106930A4400&LanguageCode=en&DocumentPartId=&Action=Launch&_ga=2.245110470.2137303789.1676448872-2043381333.1675944936*	
[11]	*Device Security Assurance Center (DSAC)* *https://library.e.abb.com/public/03f77d8934134c72865f88cc61b59798/ABB_Device_Security_Assurance_Center(DSAC)_9AKK107680A9866.pdf*	
[12]	White paper - Differentiation of the IT security standard series ISO 27000 and IEC 62443 (abb.com)	

Drive firmware manuals		
[13]	*ACS880 primary control program firmware manual*	*3AUA0000085967*
[14]	*ACS580 standard control program firmware manual*	*3AXD50000016097*
[15]	*ACS380 machinery control program firmware manual*	*3AXD50000029275*
[16]	*ACH580 HVAC control program firmware manual*	*3AXD50000027537*

Option manuals and guides		
[17]	*FEIP-21 Ethernet/IP adapter module user's manual*	*3AXD50000158621*
[18]	*FMBT-21 Modbus/TCP adapter module user's manual*	*3AXD50000158607*
[19]	*FPNO-21 PROFINET fieldbus adapter module user's manual*	*3AXD50000158614*
[20]	*NETA-21 remote monitoring tool user's manual*	*3AUA0000096939*
[21]	*Drive composer start-up and maintenance PC tool User's manual*	*3AUA0000094606*
[22]	*Ethernet tool network for ACS880 drives application guide*	*3AUA0000125635*

You can find manuals and other product documents in PDF format on the Internet. See section *Document library on the Internet* on the inside of the back cover. For manuals not available in the Document library, contact your local ABB representative.

Further information

Product and service inquiries

To report a suspected problem or to get the latest information about cyber security, please visit the ABB Cyber security Portal or send an email:

Web: https://global.abb/group/en/technology/cyber-security

Email: cyber security@ch.abb.com

Publicly disclosed vulnerability public responses can be found from ICS-CERT - https://ics-cert.us-cert.gov/alerts.

Product training

For information on ABB product training, navigate to https://new.abb.com/service/training.

Providing feedback on ABB manuals

Your comments on our manuals are welcome. Navigate to https://new.abb.com/drives/manuals-feedback-form.

Document library on the Internet

You can find manuals and other product documents in PDF format on the Internet at https://library.abb.com/.

Contact us

www.abb.com/drives

www.abb.com/drivespartners

3AXD10000492137 Rev C (EN) 2023-04-14

Power and productivity
for a better world™