ABB drives

Technical guide
Cybersecurity for ABB drives

Power and productivity
for a better world™

List of references

General guides		Code (English)
[1]	*ABB 670 series IEC 2.0 Cyber Security Deployment Guideline*	*1MRK 511 309-UEN*
[2]	*ABB System 800xA Extended Cyber Security*	
[3]	*ESCoRTS Project (European network for the Security of Control and Real-Time Systems)*	
[4]	*NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security*	
[5]	*IEC 62443 series standards, Industrial communication networks – Network and system security*	

Drive firmware manuals		
[6]	*ACS880 primary control program firmware manual*	*3AUA0000085967*
[7]	*ACS580 standard control program firmware manual*	*3AXD500000160697*
[8]	*ACS380 Machinery control program firmware manual*	*3AXD50000029275*
[9]	*ACH580 HVAC control program firmware manual*	*3AXD50000027537*

Option manuals and guides		
[10]	*FENA-01/-11/-21 Ethernet adapter module user's manual*	*3AUA0000093568*
[11]	*NETA-21 remote monitoring tool user's manual*	*3AUA0000096939*
[12]	*Drive composer start-up and maintenance PC tool User's manual*	*3AUA0000094606*
[13]	*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.

Technical guide

Cybersecurity for ABB drives

Table of contents

3AXD10000492137 Rev A
EN
EFFECTIVE: 2016-06-09

Table of contents

1. Introduction to the guide

2. Cybersecurity essentials

3. Cybersecurity standards

4. Example cases

5. ABB cybersecurity policies

Further information

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 in achieving a better understanding of cybersecurity, typical cybersecurity challenges, and the measures required to protect the reliability, integrity, and availability of variable speed drive systems against unauthorized access or cyberattacks. The aim of the document is to introduce ABB Drives cybersecurity policies and to help in answering questions and concerns relating to cybersecurity. The document can be also used as a generic cybersecurity 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 of 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.

Glossary

Terms and abbreviations used in this guide.

Term or abbreviation	Explanation
2G, 3G, 4G	The second, third and fourth generations of mobile telecommunications technology
Access account	Access control function that allows the user access to a particular set of data or functions for certain equipment
Access control	Protection of system resources against unauthorized access
Accountability	Property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions
APN	Access point name is the name of a gateway between a GSM, GPRS, 3G or 4G 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
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
Cybersecurity objective	Aspect of security whose purpose is to use certain mitigation measures, such as confidentiality, integrity, availability, user authentication, access authorization, accountability, etc.
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
DMZ	Demilitarized zone. A physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet
DNS	Domain name system
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

Term or abbreviation	Explanation
FW	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	Hardening is 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
IDS	Intrusion detection system. A device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station
IEC	International Electrotechnical Commission
IED	Intelligent electronic devices
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
ISA	International Society of Automation
ISMS	Information security management system. A set of policies concerned with information security management or IT related risks
ISO	International Organization for Standardization
ISO 27K	ISO 27000 series of standards
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.

Term or abbreviation	**Explanation**
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
Patch management	Area of systems management that involves acquiring, testing and installing multiple patches (code changes) to an administered computer system
PBX	Private branch exchange. A telephone exchange or switching system that serves a private organization and performs concentration of central office lines or trunks and provides intercommunication between a large number of telephone stations in the organization
PKI	A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates and manage public-key encryption.
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
RTU	Remote terminal unit
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

2

Cybersecurity essentials

Contents of this chapter

This chapter describes the essentials of cybersecurity.

Introduction

Traditionally, “cybersecurity” has been defined to mean all measures taken to protect a computer or computer system 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 unauthorized access or attack.

Cybersecurity 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 of data, both in transit and at rest.

Cybersecurity has become 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 based more and more on software.
- DoS (denial-of-service) attacks and malware (eg, worms and viruses) have become all too common and have already impacted ICS (industrial control systems).
- Computer systems now 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.

According to one definition the cybersecurity of industrial control systems typically includes three threat categories:

- **Hacking**. An attacker specifically targets an industrial control system in order 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 cybersecurity. However, these types of attacks only constitute a minority of all incidents. General malicious software and employee mistakes make up the majority of incidents.

In the next few sections, the basic protection approaches are introduced.

Defense in depth

There is no single solution to managing the cybersecurity 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. It is also known as the “castle approach,” referring to a medieval castle, which has multiple defenses (walls, one entry point, castle inside castle, moat, etc.) arrayed against identified threat vectors. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited.

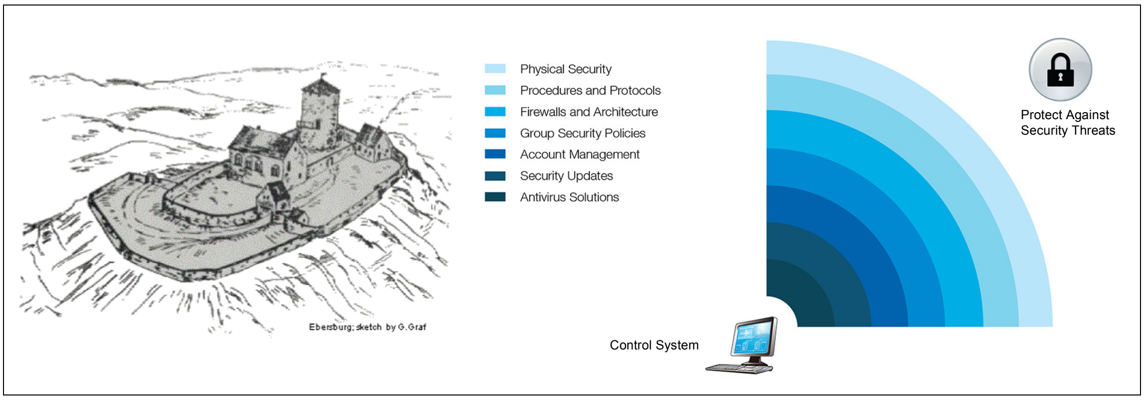

Figure 1. A medieval castle as an example of defense-in-depth and multi-layered protections [2].

The idea behind the defense-in-depth approach is to defend a system against any particular 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 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 (eg, 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.

The following example is taken from *NIST Special Publication 800-82, Guide to Industrial Control Systems (ICS) Security* [4], which introduces a model for defense-in-depth architecture in corporations that have various industrial control and automation systems around the globe. (See the figure below.)

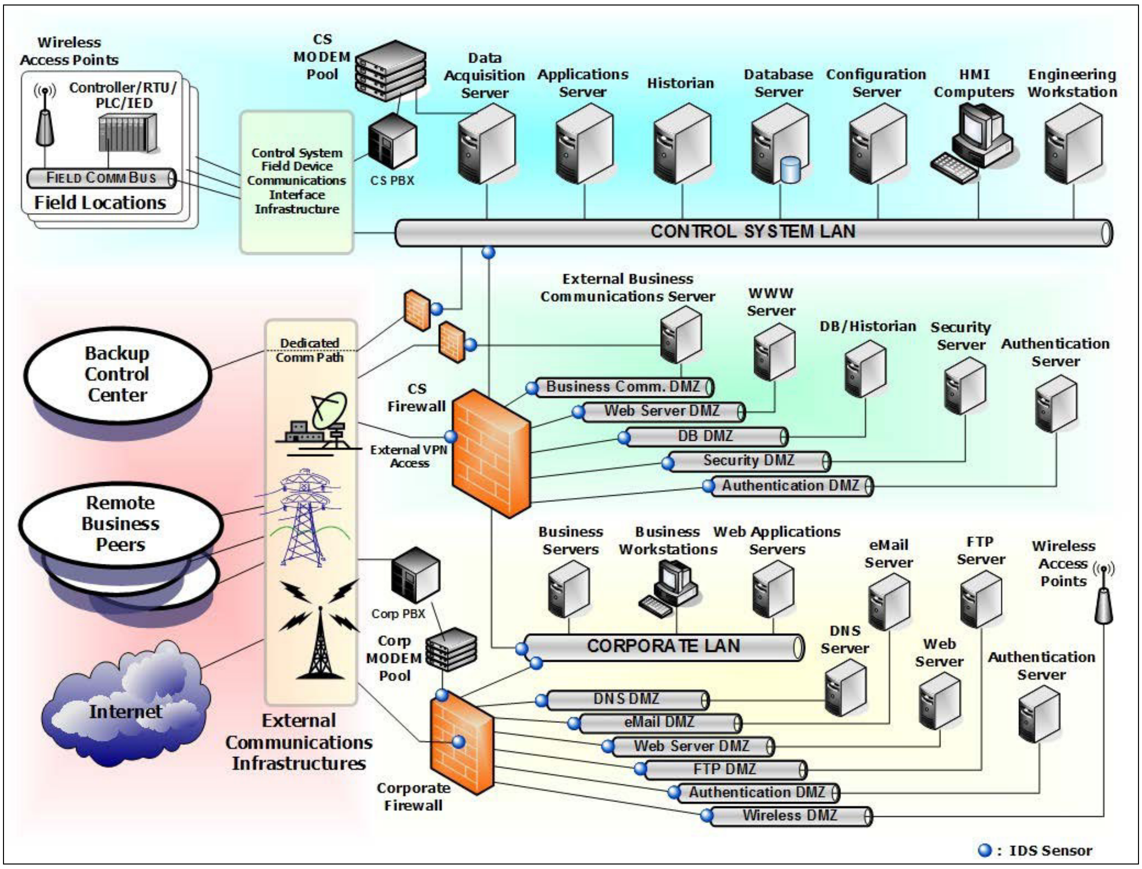

Figure 2. Defense-in-depth architecture as shown in [4].

In the defense-in-depth architecture, the control system LAN (local area network) is clearly separated from other corporate networks with firewalls, and there are separate demilitarized zone (DMZ) areas for each function, such as for historian, security and authentication. The segmentation inside the control system LAN is not visible, but also that part clearly requires more and more cybersecurity controls as of today. In other terms, there is a need to add network-level access control mechanisms, such as firewalls and managed switches, to be able to restrict unauthorized access to automation networks, devices and data.

Generic risk reduction methods and cybersecurity policies

The majority of cybersecurity risks can be controlled by feasible network architectures, access control and physical security mechanisms. Undisturbed security and management also requires a strict cybersecurity policy and approach that includes various viewpoints and activities to keep up the targeted level of cybersecurity in automation.

The basic risk reduction methods and cybersecurity policies are listed below:

- Physical security mechanisms
    - Tamper detection of unauthorized access (for example, inspecting sealing)
    - 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)
- Electronic access control
    - Firewalling the external access, which should deny any access from unauthorized parties
    - Account-based electronic access control
    - Encryption of remote access data in transit
- Network architectures and protocols
    - Segmented network solution architecture with separated automation segments
    - Segmentation of data networks into independent subnetworks that minimize any problem propagation
    - Allocating secure gateways and DMZs that enable application-level control
    - Site and automation firewalls in use with appropriate maintenance
    - Virtual private network (VPN) solutions for remote access and strict access control
    - Cryptographic protocols and algorithms for securing data communication using authentication, integrity and confidentiality protection, and replay protection
- Cybersecurity procedures and policies
    - Background checks, instructions and training of personnel and subcontractors
    - Guides on what actions are permitted, using which tools, by whom, and when
    - Logging and cybersecurity monitoring methods in automation systems and networks
- Computer policies
    - Backup and update in use and recovery tested
    - Endpoint protection in use with appropriate maintenance
    - Allowed applications specified and others removed
    - Media encryption solution in use
- Account management
    - Authentication methods before devices, software or users get access to the network
    - Access account management process in use and roles defined
    - Removal procedure for default accounts and passwords
- Patch management
    - Managed installation of software and security patches, including change management

Cybersecurity solutions are reaching almost all automation applications. The concept of the “trusted network” remains useful. The “trusted network” should be understood, from a cybersecurity 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 cybersecurity procedures and policies are always required.

The cybersecurity 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 upgrading. 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 cybersecurity products and features, which may not guarantee correct operation under all circumstances. So, not all complex IT security tools can be used in automation.

Automation networks

Today fieldbus connectivity is also often a gating requirement for acceptance as a drives 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) none of standardized industrial fieldbuses support authentication or any other basic cybersecurity methods. 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 cybersecurity protection, but the change will take time.

As stated earlier, often it is not easy to upgrade certain control systems, and all upgrades 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 and commissioning of the communication interface, eg, the fieldbus interface of a drive. That is, drives are typically not network-enabled or network-connected by default.

Cybersecurity versus safety

Cybersecurity in automation aims for retaining a continuous operation. This means that the safety and operational continuity requirements become first, and the cybersecurity requirements follow these. 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.

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

The cybersecurity objectives are subordinate to safe operation requirements. The identification of cyberattacks, industrial espionage and malicious and unauthorized software are important subordinate goals.

Roles and responsibilities

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

These are examples of partners and their roles ensuring valuable cybersecurity co-operation:

- **Systems integrators**. Competence in and experience of integration challenges, possible platform weaknesses and cybersecurity bottlenecks in system integration.
- **Telecommunication network operator**. Establishing and cybersecurity monitoring of private access points and possibly VPNs for customers.
- **Office security services**. Physical access control and monitoring of facilities, rooms, cabinets, etc.
- **Automation vendor**. Validation and approval of all cybersecurity solutions, before their actual commissioning in the field. Adviser on secure usage of devices and applications, upgrades, patches, maintenance and monitoring services, etc.
- **Network equipment vendor and LAN operator services**. Establishing and maintaining a secure network architecture together with managed switches (VLANs), routers (networks), firewalls (access control), and monitoring services (identification of malicious behavior or software).
- **Software providers**. Maintenance of operation system software, antivirus software, management software, etc.

Generic cybersecurity solutions

Automation system operation can fail totally due to the reason that cybersecurity 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 eg, hacking tools and methods may be needed.

Cybersecurity levels and their accompanying requirements help to understand whether cybersecurity is covered sufficiently in a project or in an operational automation service. Good examples of cybersecurity requirements and levels can be found in IEC 62443-3-3, *System Security Requirements and Security Levels* [5] (see chapter *Cybersecurity standards*). Requirements should be applied according to identified threats.

The targeted cybersecurity 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 cybersecurity 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.

Cybersecurity must be considered in all phases. Otherwise, the risk can find its way to the target without notice. The table below lists typical cybersecurity considerations in different project phases.

Phase	**Cybersecurity activity**
Development & pilot phases	Install the firewalls and remote access (VPN) solution according to company policy and cybersecurity requirements.
	Enable remote access only for authorized vendor personnel with authorized user accounts.
	Restrict (each user account) access from different vendors to subnetworks or machines belonging to the delivery.
	Install trusted signed SW packages only from trusted sources (eg, from ABB Drives site with HTTPS).
	Install vendor-approved patches.
Commissioning phase	Hardening of systems. Check and ensure that there is a specific cybersecurity 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.
	Test that all systems and cybersecurity mechanisms work according to the specifications.
	Communicate to all users and train them in the established cybersecurity and change management procedures.
	Establish network cybersecurity monitoring systems and ensure that these cannot negatively affect the system operation under any circumstances.
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 operation systems.
	Monitor the system logs for unauthorized access or other suspect behavior.
	Plan and test system upgrades and new features in test facilities before applying them to production systems.

3

Cybersecurity standards

Contents of this chapter

This chapter describes standards related to cybersecurity.

Cybersecurity standards in automation

ABB recognizes the importance of cybersecurity 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.

In general, the most important cybersecurity standards in automation are:

- IEC 62443 series: *Industrial communication networks – Network and system security*
- NIST 800-53: *Security and Privacy Controls for U.S. Federal Information Systems and Organizations*
- NIST Cybersecurity Framework: Framework for Improving Critical Infrastructure Cybersecurity
- NERC CIP: Critical Infrastructure protection standards
- ISO 27000-series: The ISO 27000 series of standards for all information security matters
- IEEE P 1686: *IEEE Draft Standard for Substation Intelligent Electronic Devices (IED) Cyber Security Capabilities*
- IEC 62351: Standards for information exchange for power systems and other related systems including Energy Management Systems, SCADA, distribution automation & tele protection

The available standards, frameworks and regulations are mapped as shown in *Figure 3*. They are mapped according to their relevance for operators and manufacturers and also according to whether they cover technical or management/process/policy aspects.

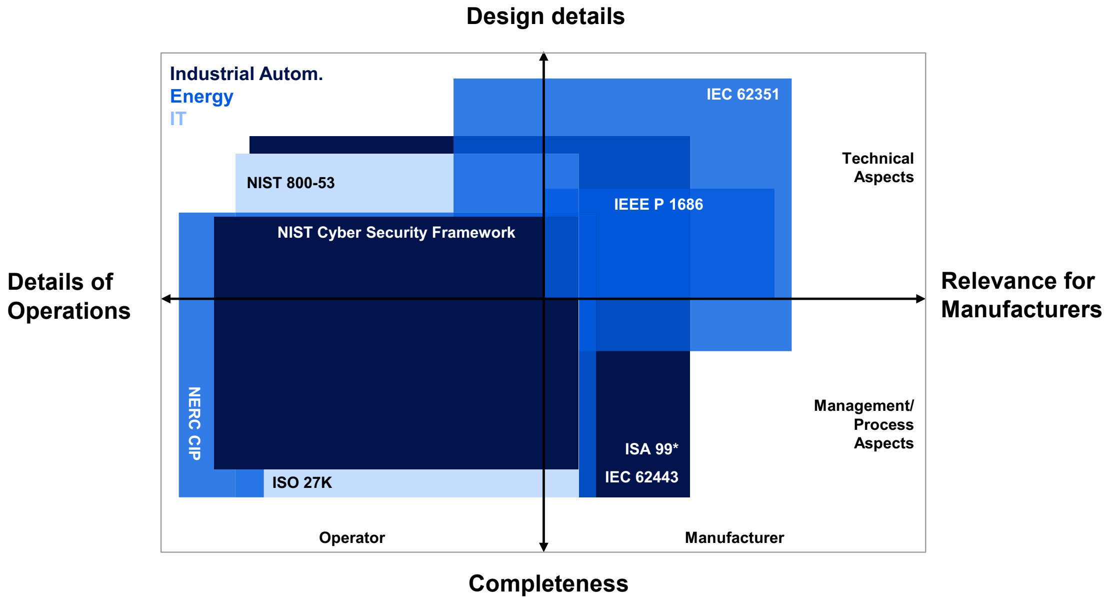

*Figure 3. Important cybersecurity standards and their scopes. *)Since the closing of the ESCoRTS project, ISA decided to relabel the ISA 99 standard as ISA 62443 to make the alignment with the IEC 62443 series more explicit and obvious. [2], [3], [4], [5]*

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

The main reference for automation cybersecurity requirements is documented in standard IEC 62443 (also known as ISA 99) with the widest scope and most detailed guidelines [5]. The NIST Cybersecurity Framework version 1.0 was published on February 1, 2014 and has less details. 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 the table below.

IEC Reference	Title and scope
IEC/TS 62443-1-1	Terminology, concepts and models for industrial automation and control systems (IACS) security
IEC/TR 62443-1-2	Master glossary of terms and abbreviations
IEC 62443-1-3	Identifies a set of compliance metrics for IACS security
IEC/TR 62443-1-4	IACS security life cycle and use cases
IEC 62443-2-1	Requirements for an IACS security management system
IEC/TR 62443-2-2	Implementation guidance for an IACS security management system
IEC/TR 62443-2-3	Patch management in IACS environments
IEC 62443-2-4	Focuses on the certification of IACS supplier security policies and practices

IEC Reference	Title and scope
IEC/TR 62443-3-1	A technical report on the subject of suitable technologies for IACS security
IEC 62443-3-2	Security risk assessment and system design
IEC 62443-3-3	System security requirements and security levels
IEC 62443-4-1	Product development requirements
IEC 62443-4-2	Detailed technical security requirements for IACS components

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

4

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 cybersecurity point of view and secure deployment practices, that is, generic resolution and mitigation of identified cybersecurity 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 a large number of 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 of the necessary details for implementing a secure system. As far as deployment of ABB drive and connectivity products, all guidelines and instructions are real and valid though.

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, ABB ACS880 industrial drives are used to represent variable speed drives. The other ABB Drives connectivity and software products shown are:

- AC500 / AC500-S Safety PLC (programmable logic controller)
- FENA-11/-21: Ethernet adapter module − allows Ethernet communication for drives
  - FENA-11 and -21 support industrial Ethernet protocols (Modbus/TCP, Ethernet/IP and PROFINET IO) that do not specify cybersecurity features
- NETA-21. Remote monitoring for drives
  - Implements security features for communicating over untrusted networks
  - Includes user authentication, user accounts, and secure communication.
- Automation Builder with Drive Manager plug-in. Integrated software suite for machine builders and system integrators to automate their machines and systems
  - Combines the tools required for configuring, programming, debugging and maintaining automation projects from a common interface
- Drive composer. Software tool for start-up and maintenance of ABB's common architecture drives
  - Used to view and set drive parameters, and to monitor and tune process performance.

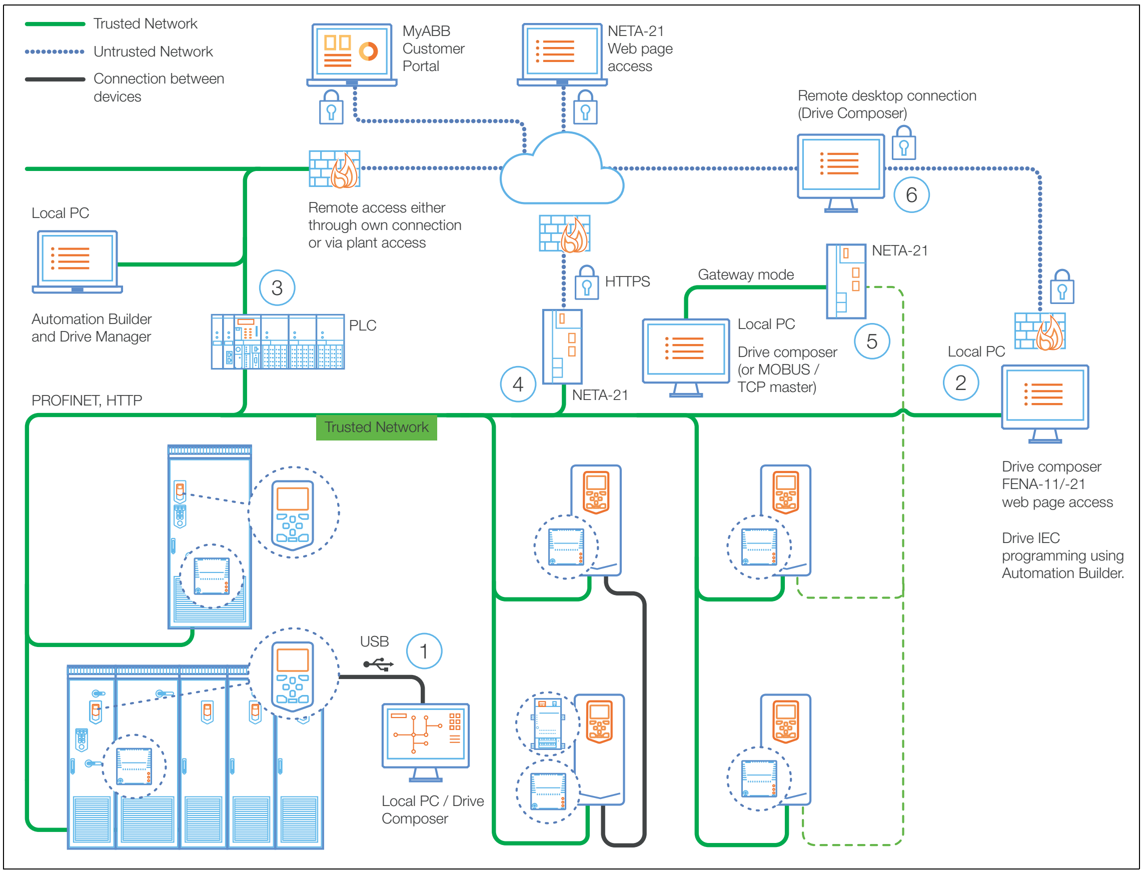
Trusted Network
Untrusted Network
Connection between devices
MyABB Customer Portal
NETA-21 Web page access
Remote desktop connection (Drive Composer)
Local PC
Remote access either through own connection or via plant access
6
3
NETA-21
Gateway mode
HTTPS
Automation Builder and Drive Manager
PLC
Local PC
5
Drive composer (or MOBUS / TCP master)
4
NETA-21
Local PC
2
PROFINET, HTTP
Trusted Network
Drive composer FENA-11/-21 web page access
Drive IEC programming using Automation Builder.
USB
1
Local PC / Drive Composer

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 Drive composer start-up and maintenance tool and/or Automation Builder suite tool via
  1. local connections (point-to-point serial communication, ie, USB) or
  2. shared (with control) upper-level physical fieldbus network (eg, PROFINET) using Ethernet tool communication and/or
  3. communicating also through PLC system using Drive Manager device tool or
  4. NETA-21 remote monitoring tool web interface or
  5. NETA-21 acting as a gateway between or
  6. third-party remote desktop connection.
- **Maintenance and troubleshooting** using the aforementioned tools and communication networks
- **Remote support and remote condition monitoring** services
- **On-demand based remote monitoring** over untrusted network (public Internet) using the NETA-21 remote monitoring tool

The architecture illustrated includes the following components:

- In the public networks, there are services such as:
  - MyABB Customer Portal (cloud service)
  - Remote monitoring via web page access, eg, NETA-21 remote monitoring tool.
  - Remote desktop connections (Drive composer)
- 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 (eg, PROFINET) via FENA-11/-21
  - Drives that are connected to a local PC via USB
  - NETA-21, that is also connected to public networks via firewall
  - NETA-21 that is connected to the drives with EIA-485 and to a local PC using gateway mode

Cybersecurity 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 FENA-11/-21 deployment

FENA-11/-21 must be positioned in a trusted network (strictly limited and well hosted portion of a network or control system)

On the FENA-11/-21 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 FENA-11/-21 web pages
- Change of IP settings remotely using ABB IP configuration tool
- Remote access to drives with Drive composer tool via Ethernet tool network
- Ping response

For more information, see *FENA-11/-21 user manual* [10].

ACS880 industrial drives deployment

User lock. For better cybersecurity, it is possible to set a master password to prevent eg, 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
- safety functions module (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
- configuration settings available through control panel such as time/date formats and enabling/disabling clock display.

User access levels. Configure for local user interfaces (Drive composer and control panels) parameter access rights using parameter lock feature.

For more information, see *ACS880 primary control program manua*l [6].

Drive composer PC tool Ethernet tool communication deployment:

Drive composer establishes Ethernet communication only with “recognized devices”, that is, FENA-11/-21 Ethernet fieldbus adapters. This is the default mode of operation.

For more information, see *Ethernet tool network for ACS880 drives application guide* [13].

NETA-21 deployment

Configure the cybersecurity features of NETA-21 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 NETA-21 tool is being used, to have the latest software versions and security patches in use.

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): disable the SSH service (factory support account) when SSH console for support and diagnostics is not needed.
- Locale settings: disable NTP (Network Time Protocol) requests that NETA-21 can send to external servers, or replace with local NTP time servers if such are available.
- 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 NETA-21 within local network

If NETA-21 and Drive composer are used at the same time over Ethernet, the PC tool-friendly mode should be used in NETA-21.

Actively monitor the internal network. Specifically track for any unauthorized devices.

For more information, see *NETA-21 remote monitoring tool user’s manual* [11] and *Ethernet tool network for ACS880 drives application guide* [13].

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.

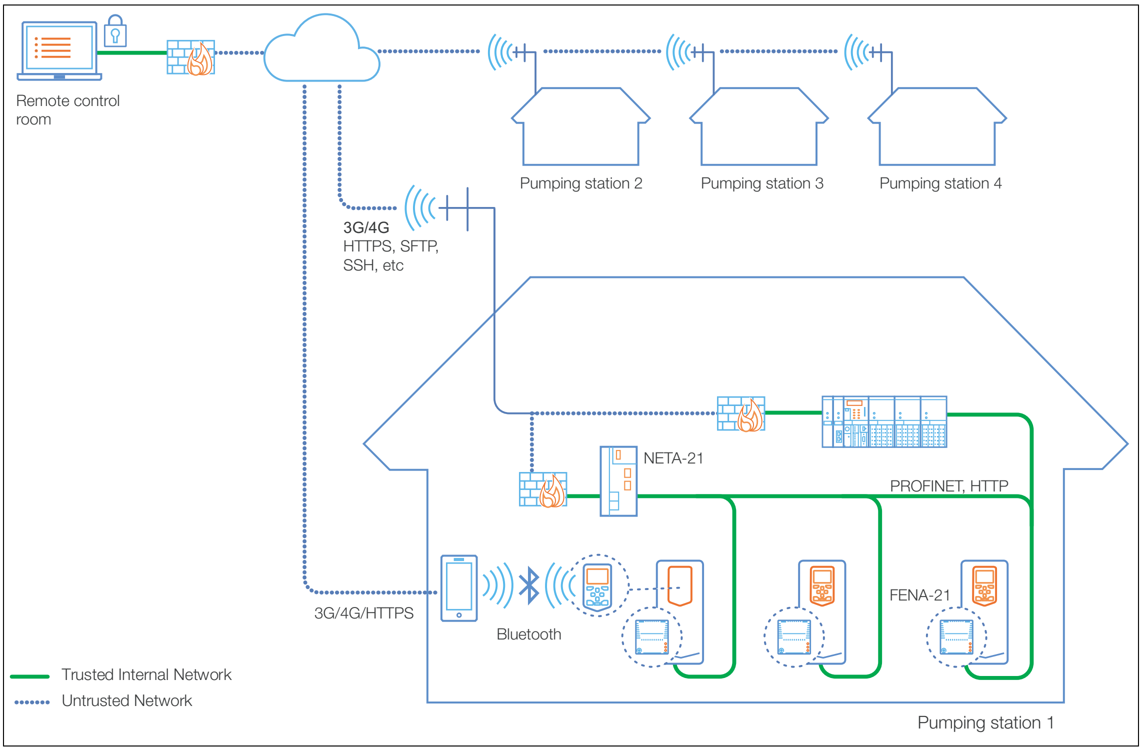

Figure 5. Water Pumping Station with permanent wireless connections.

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 cybersecurity point of view, this approach increases the number of field automation devices and cybersecurity-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 has the result that the local network cannot be stated as trusted and implies that defense in depth must be implemented.

Cybersecurity 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 cybersecurity 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: manage carefully all firewalls, their configurations and access rules.

ACS580 general purpose drive deployment:

See section *Cybersecurity risk mitigation and secure deployment* on page *28* for deployment instructions for the ACS880. Follow the same procedures. [7]

Ethernet fieldbus adapters FENA-11/-21 deployment:

See section *Cybersecurity risk mitigation and secure deployment* on page *28* for deployment instructions for FENA-11/-21. Follow the same procedures. [10]

Drive composer PC tool Ethernet tool communication deployment:

See section *Cybersecurity risk mitigation and secure deployment* on page *28* for deployment instructions for FENA-11/-21. Follow the same procedures. [13]

Drivetune, ACS-AP-W assistant control panel and Bluetooth connection deployment:

- Disable “always discoverable” mode when configuring the Bluetooth connection in case it is not needed. The always discoverable mode keeps the ACS-AP-W assistant control panel discoverable to any Bluetooth device within wireless range.
- If 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.

NETA-21 deployment:

Configure the cybersecurity features of NETA-21 similarly to the first case. See section *Cybersecurity risk mitigation and secure deployment* on page *28* for more detailed deployment instructions for NETA-21.

Case 3 – Machinery OEM Equipment

Description

This example case is similar to 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 also 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.

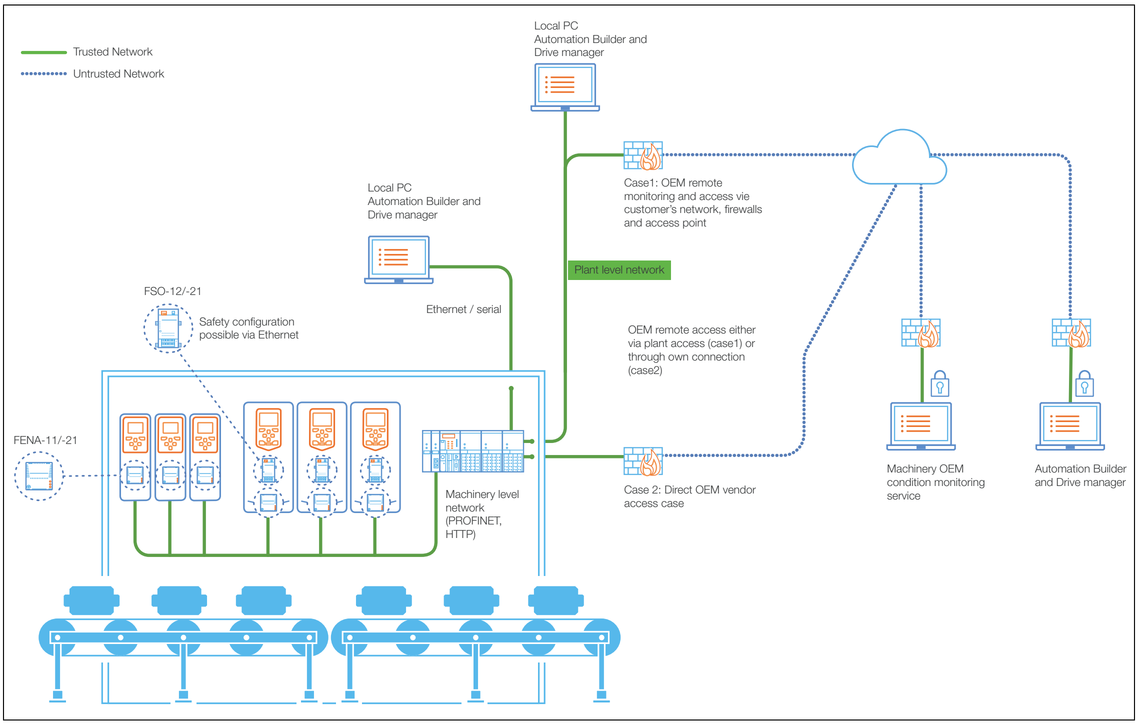
Trusted Network
Untrusted Network
Local PC
Automation Builder and
Drive manager
Case1: OEM remote monitoring and access vie customer's network, firewalls and access point
Local PC
Automation Builder and
Drive manager
Plant level network
FSO-12/-21
Safety configuration possible via Ethernet
Ethernet / serial
OEM remote access either via plant access (case1) or through own connection (case2)
FENA-11/-21
Machinery level network (PROFINET, HTTP)
Case 2: Direct OEM vendor access case
Machinery OEM condition monitoring service
Automation Builder and Drive manager

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 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.

Cybersecurity 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 cybersecurity 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 cybersecurity features on.
- Deny all other connectivity mechanisms from the machine-level systems to restrict unauthorized access as much as possible.
- Monitor the cybersecurity, topology (asset management) and correct operation of the plant networks using the cybersecurity 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 cybersecurity 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 cybersecurity 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.

ACS380 and ACS880-M04 machinery drive deployment:

See section *Cybersecurity risk mitigation and secure deployment* on page *28* for deployment instructions for ACS880. Follow the same procedures. [8]

Ethernet fieldbus adapters FENA-11/-21 deployment:

See section *Cybersecurity risk mitigation and secure deployment* on page *28* for deployment instructions for FENA-11/-21. Follow the same procedures. [10]

Drive composer PC tool's Ethernet tool communication deployment:

See section *Cybersecurity risk mitigation and secure deployment* on page *28* for deployment instructions for FENA-11/-21. Follow the same procedures. [12], [13]

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:

- **FBIP-21**. The FBIP-21 BACnet/IP adapter module is an optional device for ABB drives, eg, the ACH580, enabling the connection of the drive to a BACnet/IP network.
- **RBIP-01**. The RBIP-01 BACnet/IP Router Module 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.

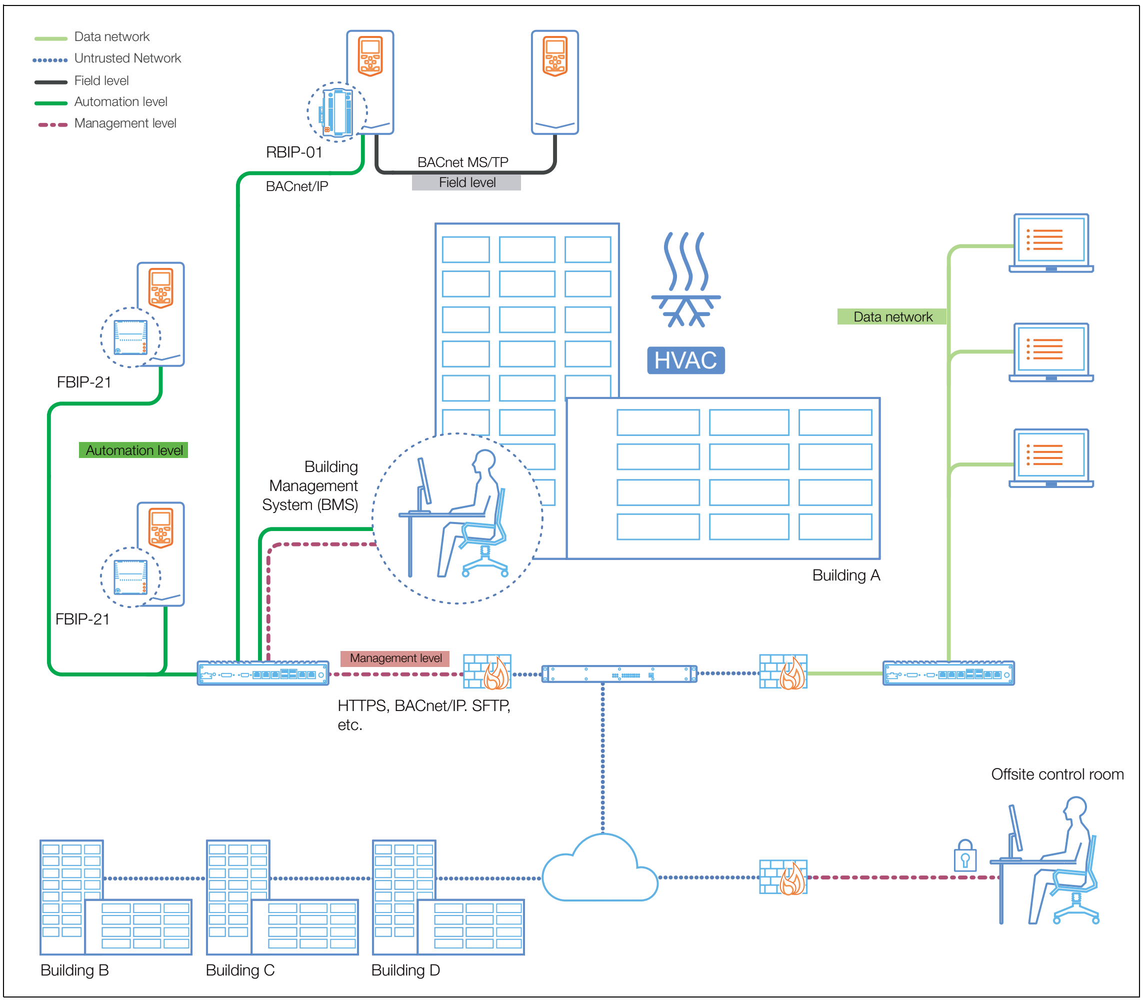

Figure 7. Building automation case.

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

Cybersecurity 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 cybersecurity 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 necessary cybersecurity features on.
- Deny all other connectivity mechanisms from the building automation systems to restrict unauthorized access as much as possible.
- Monitor the cybersecurity, topology (asset management) and correct operation of the building data networks using the cybersecurity 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.

ACH580 HVAC drive deployment:

See section *Cybersecurity risk mitigation and secure deployment* on page *28* for deployment instructions for ACS880. Follow the same procedures. [9].

5

ABB cybersecurity policies

Contents of this chapter

This chapter describes the ABB policies related to cybersecurity.

Principle

ABB Drives takes all cybersecurity-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 cybersecurity of applied technical solutions without substantially sacrificing functional safety or operational performance or productivity.

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

Device Security Assurance Center (DSAC)

ABB has defined cybersecurity 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, enabling:

- ABB to supply customers with products that meet the highest robustness standards
- ABB products and devices to comply with existing and forthcoming governmental and industrial regulations
- ABB to be a master in automation device security.
- A centralized security testing process, applying up-to-date and rigorous procedures, guarantees a common and best practice approach.

A suite of state-of-the-art open source and commercial solutions are used for testing, including device profiling, known vulnerability, denial of service and protocol fuzz tests.

Further information

Product and service inquiries

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

Web: http://www.abb.com/cybersecurity

Email: cybersecurity@ch.abb.com

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

ABB corporate-wide cybersecurity concepts, principles and secure deployment can be understood by reading eg, *ABB 670 series 1.2 Cyber Security Deployment Guideline* [1] or *ABB System 800xA Extended Cyber Security* [2].

Product training

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

Providing feedback on ABB manuals

Your comments on our manuals are welcome. Navigate to 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 www.abb.com/drives/documents.

Contact us

www.abb.com/drives
www.abb.com/drivespartners

3AXD10000492137 Rev A (EN) 2016-06-09