WHITE PAPER

Protecting operations through cyber security: ABB Drives solutions

Introduction

As network technologies advance, industry is becoming ever more connected. In industrial settings, dozens of individual drives, motors, and other machinery can be connected to networks for performance monitoring, maintenance planning, and other purposes. Industrial Automation and Control Systems (IACS) have made a big difference to many industries over the past twenty years. Operational technology equipment is supported by information technology networks to improve performance.

With this interconnectivity comes a set of concerns related to cyber security. Any Information Technology (IT) or Operational Technology (OT) network must be protected to safeguard its value - whether in terms of data, process uptime, or anything else - without forfeiting safety or control. Cyber security involves ensuring network protection is in place to combat unauthorized access or control. For ABB, cyber security affects the complete portfolio of products, systems, projects, and service deliveries. For example, ABB connected devices include built-in safety standards that ensure optimized, uninterrupted operation and are designed to meet international regulations covering cyber security risks.

This white paper describes ABB’s cyber security profile and considers how drive solutions overcome related challenges.

Differences between IT and OT cyber security

In general, the term cyber security refers to protecting computer networks against unauthorized access or attacks. Possible threats are many, from loss of intellectual property or data manipulation to process downtime or sabotage.

Cyber security has two main areas of operation. Firstly, in the case of information technology systems, it ensures the Confidentiality, Integrity, and Availability (CIA) of data. For example, customer databases held by companies must be secure from hacking attempts, malware attacks, and employee error. Data security is the priority.

Today's IT systems use standardized, commercial components. Control systems may be distributed over a wide area, which opens more attack points where the software is vulnerable. The increased number of smart devices that are connected in computer systems and network types such as WLAN, WAN, MAN, etc., demonstrate an increasingly varied installed base in many industries. This presents more possibilities for malignant actors to steal or damage data.

The reporting of distributed denial of service (DDoS) and similar attacks on IT networks of companies of all sizes is becoming more common, and the attempts more serious. The potential to profit from hacking activities has increased as machine learning Artificial Intelligence (AI) and other technologies are increasingly used by fraudsters. To protect against malicious actions and allay customer concerns over privacy and financial loss, companies need to invest more than ever in cyber security. The continuous research into AI technologies is also affecting future cyber security concerns, as governments[1] fear they will increase the risks of cyberattacks, online fraud, and replicating malware.[1]

Secondly, cyber security in operational technology (OT) applications considers process availability and safety a higher priority than data protection. In this field, the CIA order of importance is reversed to AIC – Availability, Integrity, and Confidentiality. OT cyber security presents its own challenges. Because these applications are naturally configured differently in different locations, it is hard to test updates or patches before they can be applied.

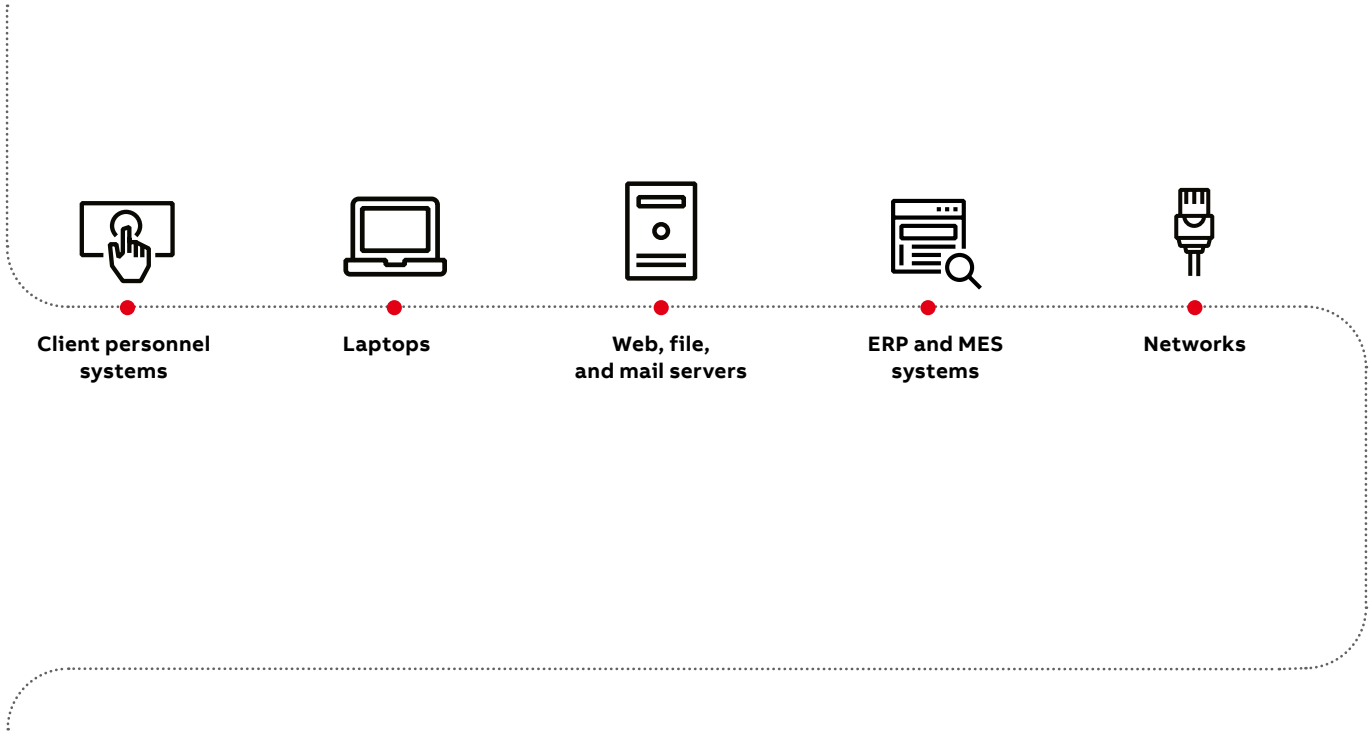
In critical applications such as power generation, it is often the case that operation cannot be paused for software updates, so critical updates to ensure integrity may not be available at all. Effective new technologies such as variable speed drives (VSD) have proliferated as fieldbus connectivity is required by customers. Originally, almost all of the standard industrial fieldbuses lacked cyber security capabilities, meaning that VSDs did not normally offer secure traffic that protected against hostile third parties. Currently, Industry 4.0 technologies such as OPC Unified Architecture[2] as well as emerging fieldbus standards have added security features.

Unfortunately, the potential risks from cyberattacks on OT have increased. Whereas OT systems used to be separate from the IT environment and the internet in general, today's variants are increasingly meshed in those networks and potentially subject to hostile action. Noted OT attacks such as the Trisis/Triton malware breach in 2017[3] or the EKANS ransomware disruption in 2020[4] have indicated how vulnerable safety instrumentation actually is, and how important developing effective security measures for critical processes and infrastructure has become.

The differences between OT and IT notwithstanding, as different industrial networks converge, security solutions must be integrated at all levels. Many of the relevant industries involve critical infrastructure such as energy, water, and transportation. Implementing effective processes, training personnel, and keeping abreast of regulatory developments present a multi-layered and complex set of cyber security challenges that are ever more common in today's automated, digital industrial networks.

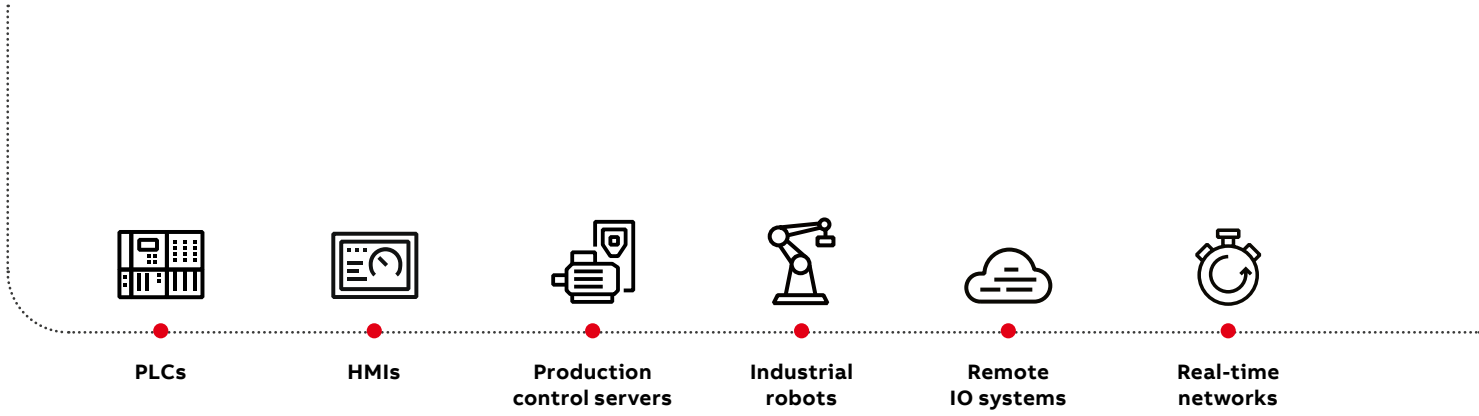
IT

Information Technology is the common term to describe information processing technologies including software, hardware, communication technologies, and related services.



OT

Operational technology is hardware or software that detects or causes a change through direct monitoring and/or controlling industrial equipment, facilities, processes and events.



—

In IT security the priorities are Confidentiality, Integrity and Availability of information. In OT security the priorities are Availability, Integrity and Confidentiality of the operations performed by the system.

Standards and regulations

The establishment of national and international cyber security standards and regulations has gathered pace over the last decades. Understanding and applying relevant requirements is demanding, as is continuously monitoring regulations for updates and changes that must also be applied, documented, and reported. But, in order to do business, organizations are bound to follow them. ABB encourages customers to consider security from a holistic standpoint where it is seen as an integral part of all connected processes rather than as a simple box-ticking exercise. This holistic approach provides immediate value when one considers that the IT and OT environments focus on different standards – mainly the ISO 27000 series and IEC 62443 series respectively, but also other prominent ones such as 3GPP[5] – even though the same network can fall under both sets. This section will highlight some of the most relevant standards and regulations in effect now and in the near future.

Standards

ISO 27000

The ISO 27000 series of standards covers information security management systems (ISMS). Information security is focussed on how to ensure the continuous confidentiality, availability, and integrity of information. Necessary processes should be identified and security risks described, assessed, and controlled.

The series consists of general guidelines specified in several standards. For example, the 27001 standard defines measures related to formalized information management systems: their introduction, implementation, operation, monitoring, review, and improvement. The 27002 standard, on the other hand, guides and provides best practices for the implementation of those specified measures.

The ISO 27001 standard includes topics such as:

- **Allocation of access rights, user administration, access administration, password and key management**
- **Disposal of data carriers**
- **Access to networks and network services**
- **Physical security**
- **Operational processes and responsibilities**
- **Protection against malware**
- **Data back-up**
- **Network security management and segregation**
- **Supplier relationships**

Guidance for auditing and risk management of information security management systems are also provided in the ISO 27000 series.

IEC 62443

The IEC 62443 series of standards is based on the requirements of the ISO 27000 series and concerns the special needs of IT and OT in the industrial communication networks and system security in the production area. The series includes parts that describe life cycle procedural requirements and their implementation for suppliers of industrial automation systems and maintenance service providers.

Basic requirements for automation systems include:

- **Authentication and Identification control**
- **Use control**
- **System integrity**
- **Data confidentiality**
- **Resource availability**
- **Restricted data flow**

Comparison of ISO 27000 and IEC 62443 standards

	Information security	Focus on	Focus	Protects
ISO 27000	In Management Systems	Information technology (IT)	Confidentiality, availability and integrity of data with adequate processes and risk management.	Information assets
IEC 62443	In production	Operational technology (OT)	Availability and safety of industrial processes through the secure design, installation, and management of automation and control systems and components.	Production, systems, and products

The IEC 62443 standard sets cyber security benchmarks in all industry sectors that use industrial automation and control systems including building automation, electric power, and process industries like chemicals or oil and gas. The IEC 62443 standard underpins the whole of ABB's cyber security programme and reference architecture.

Of particular interest to ABB Drives as a product manufacturer are parts 4-1 and 4-2. The former concerns characteristics of a secure product development process, such as security requirement definitions, design, development, testing and vulnerability handling.

The latter defines technical requirements for products or components.

The basic concepts and technologies are to be found in both sets, although the IEC 62443 series has a clear focus on automation, while the ISO 27000 series is more process-oriented and generic.

Standards are informative recommended best practices. Legislation, on the other hand, is considered normative and lack of adherence might prevent manufacturers from selling their products.

Legislation

Examples of cyber security legislation around the world

KEY EU REGULATIONS

NIS directive, second edition (NIS2)[7]
Enhances security of network and information systems within the EU.

Machinery Regulation (MR)[8]
Addresses safety of machinery, including cybersecurity of safety control systems and software.

Cyber Resilience Act (CRA)[9]
Safeguards consumers and businesses buying or using products or software with a digital component.

Radio Equipment Directive (RED)[10]
Establishes manufacturing standards for internet-connected equipment with wireless connections.

USA

Security and Privacy Controls for Information Systems and Organizations (NIST 800-53)[6]
Provides a catalog of flexible and customizable security and privacy controls for information systems and organizations.

CHINA

Cybersecurity Law of the People's Republic of China[11]
Monitors, prevents, and handles cyber security risks through the establishment of standards, technical measures, and security obligations.

How ABB Drives implement cyber security

At ABB Drives, cyber security, along with high standards of quality and safety, is embedded in everything we do. All our products are designed, manufactured, and maintained assuming the necessity of cyber security.

We use a holistic approach, where security is managed in three main contexts: Internal Operations, Product Development Processes, and Product Features.

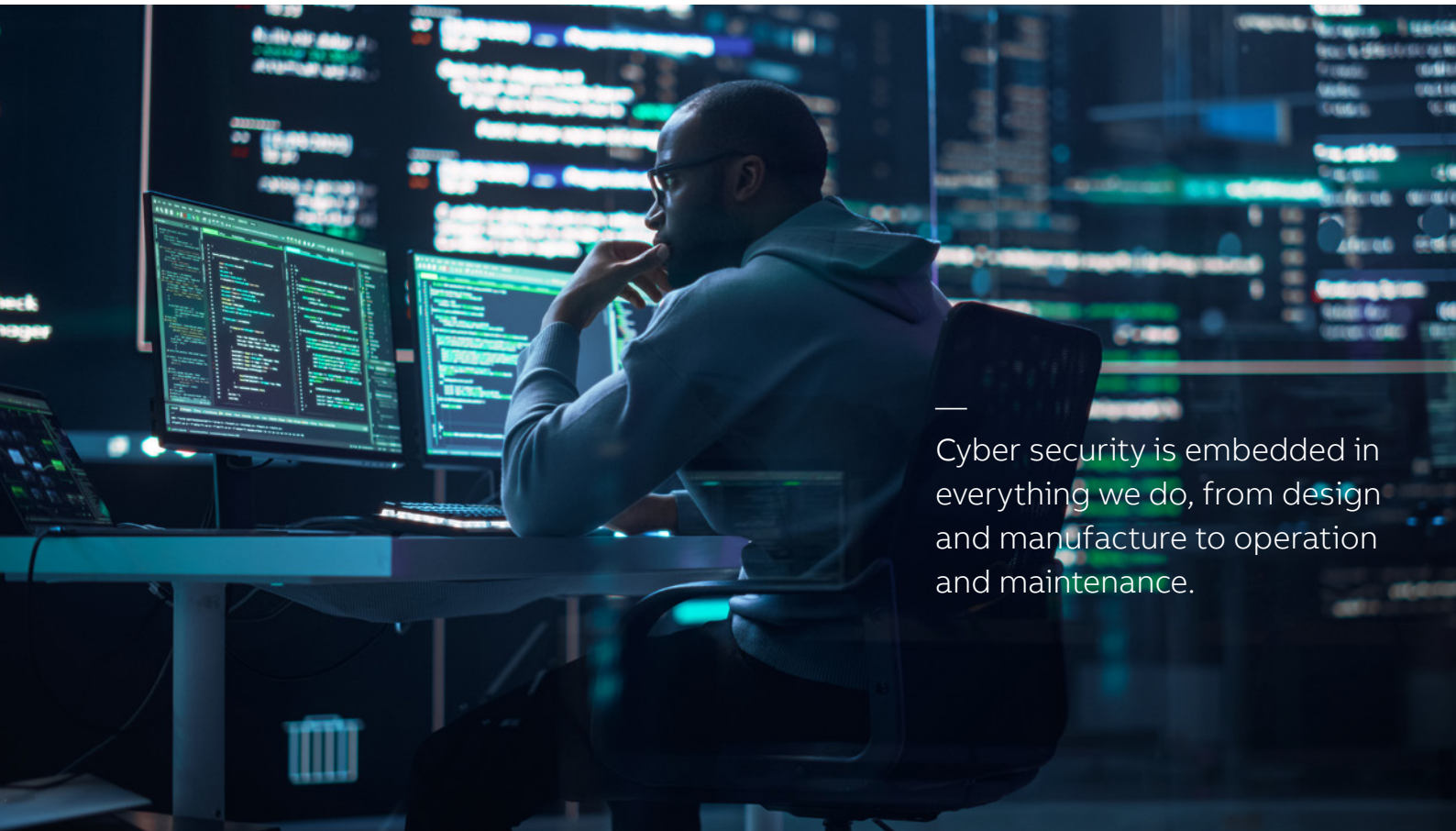
Internal Operations

In ABB's Code of Conduct[12] there is a specific section dedicated to Information and technology security[13], emphasising ABB's commitment to securing its assets, employees, partners and customers from cyberattacks.

Policies and Standards
ABB has a comprehensive set of internal policies and standards covering topics such as Information Classification and Handling, and Threat and Vulnerability Management.

End Users IT asset usage
ABB security policies are aligned with the most relevant security regulations and standards both globally and regarding specific industries. The policies are continuously updated to ensure their continued compliance.

Awareness and Training Programs
To encourage a secure culture within our organization and promote healthy security habits amongst all ABB employees, we promote relevant knowledge during live training sessions, e-learnings, security articles, videos, blog posts, podcasts, and so on.



Cyber security is embedded in everything we do, from design and manufacture to operation and maintenance.

Product Development Processes

ABB Drives organization adopts a comprehensive approach to cyber security in all stages of the Secure Development Life Cycle, following IEC 62443-4-1.

1

Security Management.
A comprehensive set of documented processes certified against ISO 9001 and IEC 62443-4-1 is shared across all sites and teams of the ABB Drives organization. Engineers are regularly trained. Software and electronic hardware suppliers must be compliant with ABB Cyber Security Requirements for Suppliers[14].

2

Security Requirements.
This involves a rigorous and systematic management of security features and bugs, tracked from requirement creation to validation and release.

3

Security by design.
The extensive use of threat modelling and adoption of the most secure architectural approaches for given technologies enable secure-by-design products.

4

Secure Implementation.
We reach this by applying secure coding standards and performing static code analysis on all source code.

5

Security verification and validation testing.
The ABB DSAC (Device Security Assurance Center)[15] which has been IEC 62443-4-1 ML-3 certified by Exida[16] validates drive security and performs penetration testing.

6

Management of security-related issues.
Proper and timely handling of 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 is described in this document[17].

7

Security update management.
We continuously keep our software secure by releasing new FW/SW versions that fix security issues and improve overall performance. Customers can subscribe to Cyber security alerts and notifications[18] to be always up to date with the latest security alerts about ABB products.

8

Security guidelines.
HW, FW and security manuals are produced for all our products.

Product Features

Among the most important security features implemented in ABB Drives Next Generation portfolio are:

SECURE PROTOCOLS

A protocol is considered secure when authenticity, integrity and confidentiality are ensured. In the industrial automation world, it is not always possible to only use secure protocols, because Industrial Automation Control Systems were originally designed to be connected to trusted networks.

ABB's cloud gateway offerings such as the NETA-21[19] remote monitoring tool communicate with the ABB Ability Cloud where secure protocols have been applied to prevent unauthorized access from the cloud to the drive control.

It should be noted that secure versions of the most common fieldbus protocols have been specified. For example CIP Security for EtherNet/IP[20].

SECURE BOOT

Secure Boot is a process that runs at drives startup and prevents the loading of firmware images that are not signed with a valid digital signature.

Audit Log
The audit log is a chronological record of system activities, including records of system accesses and operations performed in a given period of time. This is important in order to reconstruct and examine a sequence of events and/or changes in an event.

Code Signing
To ensure that only trusted and original ABB software is run on the drives, binaries are signed and can be verified before starting the upgrade.

Encryption
When encryption is needed, only standard and commonly accepted cryptographic algorithms and techniques are used.

Cloud applications and services are ISO 27001 certified and aiming at C-STAR compliance. For more information, please refer to this document[21].

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 antivirus 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.

Conclusion

The importance of cyber security continues to grow as the industrial landscape evolves. With ever more interconnectivity, preventing unauthorized access and control of networks is a challenge that is already faced by all industries no matter where they are located. For ABB, the adoption of a holistic approach to cyber security, whereby it is integrated across IT and OT sectors while also meeting stringent global standards such as ISO 27001 and IEC 62443, pays the greatest dividends in securing our customers' operations and processes from malicious actors. This is not only a matter of complying with regulations but is a fundamental part of our cyber security strategy.

This strategy is realized in ABB Drives solutions through the application of key security features as described in this white paper, which together enable our customers and us to adhere to relevant security legislation. The approach taken by ABB emphasizes the criticality of cyber security in product design, development, and management. We believe present and emerging threats are best combatted by taking a proactive stance to cyber security, emphasizing innovation, and collaborating to develop industry initiatives.

1 **Certify** ABB Drives organizations and products to international cyber security standards

2 **Adopt** security controls in ABB's internal operations

3 **Apply** practices in product development as per IEC 62443-4-1

4 **Implement** security features in ABB Drives portfolio in accordance with IEC 62443-4-2

5 **Support** stakeholders in the realization of secure systems/ solutions

References

1 HM Government, "Safety and Security Risks of Generative Artificial Intelligence to 2025"
2 OPC Unified Architecture
3 "Triton: hackers take out safety systems in 'watershed' attack on energy plant", The Guardian, 2017.
4 "Honda's global operations hit by cyber-attack", BBC, 2020
5 3GPP Mobile Broadband Standards
6 Security and Privacy Controls for Information Systems and Organizations (NIST 800-53)
7 NIS2 European Cybersecurity Directive
8 European Machinery Regulations
9 European Cyber Resilience Act
10 European Radio Equipment Directive
11 Cybersecurity Law of the People's Republic of China
12 ABB's Code of Conduct
13 ABB's Code of Conduct: Information and technology security
14 ABB Cyber Security Requirements for Suppliers
15 Device Security Assurance Center
16 ABB IEC 62443-4-1 ML-3 certification
17 ABB's approach to software vulnerability handling
18 Cyber security alerts and notifications
19 NETA-21 Remote monitoring tool
20 CIP Security for EtherNet/IP
21 ABB Ability digital services for drives

Author of this document and Document owner
ABB Switzerland Ltd.
Bruggerstrasse 66
CH-5400 Baden, Switzerland

Document name
Cyber security whitepaper for ABB Drives
Document number
9AKK108469A4323
Release date
06.05.2024