WHITE PAPER

Cyber security in the AC500 PLC family

Approach cyber security with confidence

Contents

1. Objective / Introduction[1]

ABB offers a comprehensive range of scalable PLCs and robust HMI control panels. Since its launch in 2006, the AC500 PLC platform has achieved significant industry recognition for delivering high performance, quality and reliability.

In this paper, we will share insights to enhance your understanding of the ways in which customers can secure their AC500 PLC and CP600 HMI systems. Further, we offer recommendations for customers to improve their cyber security of different protocols. These hints help to reduce risks.

2. Requirements (Understanding the product design)

2.1. IEC62443-4-1 - Secure Product Development Lifecycle

We are pleased to announce that TÜV SÜD has certified the site ABB AG in Heidelberg in accordance with the **IEC 62443-4-1:2018** standard. The certificate confirms that CoE PLC Products develops Secure-by-design products. It can be found here:

- Certificate

The secure development life cycle includes:

- Definition of security requirements
- Secure design
- Secure implementation (including coding guidelines)
- Verification and validation
- Defect management
- Patch management
- Product end-of-life

2.2. IEC62443-4-2 - Technical Security Requirements for Components

We are pleased to announce that TÜV SÜD has certified the ABB AC500 V3 and AC500-eCo V3 CPUs controller family in accordance with the IEC 62443-4-2:2019 standard.

The certificate is a confirmation that the controllers of the AC500 V3 product family fulfill the security requirements for components according to the IEC 62443-4-2.

The certificate can be found here:

- Certificate

The security level capabilities of the certified product can be found here:

- Capabilities

This certificate covers seven foundational requirements:

- Identification and authentication control
- Use control
- System integrity
- Data confidentiality
- Restricted data flow
- Timely response to events
- Resource availability

2.3. NIS2[15]

What is NIS 2?

The European Union (EU) introduced the Network and Information Security (NIS) 2 Directive in December 2022 as an update to the original EU cybersecurity rules introduced in 2016. The NIS2 Directive is legislation that modernizes the existing legal framework to keep pace with increased digitization, and an evolving cybersecurity threat landscape.

NIS2 expands the scope of EU cybersecurity rules to new sectors and entities with the goal of improving the resilience and incident response capacities of public and private entities, competent authorities, and the EU as a whole. This new directive is also a positive step for all citizens of the EU because it aims to secure the critical infrastructure that all EU citizens need and rely on.

How is ABB meeting these requirements?

At ABB, we understand the importance of cybersecurity compliance in the digital landscape. We take a proactive approach to thoroughly analyze the impact of NIS 2 on our operations to work towards compliance. We have in place policies and procedures to evaluate the effectiveness of protection measures in information security. We also promote cybersecurity culture by cultivating basic cyber-hygiene practices, providing cybersecurity training to improve organizational preparedness, and secure management of users and accounts. Some of our other compliance measures in alignment with NIS 2 are:

- Policies on risk analysis and information system security
- Incident Handling Procedures
- Business Continuity Planning

- Supply Chain Security
- Network and Information Systems Security
- Effectiveness of cybersecurity risk management
- Cybersecurity Awareness across the organization

2.4. ISO 27001 - Information security management system

The ISO27001 defines requirements for ISMSs (information security management systems). It defines the requirements for the introduction, implementation, operation, monitoring, review, maintenance, and improvement of formalized information security management systems (ISMS) in connection with the overarching business risks of an organization.

We are following the process requirements of the ISO 27001 standard, even though the organization is not formally certified.

The implementation at ABB Heidelberg covers the following aspects:

- Context of the organization
- Management leadership and commitment
- Company security policy
- An organization’s roles, responsibilities, and authorities
- Measures for dealing with risks and opportunities
- Support, communication, documentation
- Operation
- Evaluation of performance
- Improvement process

2.5. Differentiation of the IT security standard series ISO 27000 and IEC 62443

Many end users have already an ISMS according to ISO 27001. At the same time, the IEC 62443-3-3 defines specific requirements for the security of the automation domain. In order to support end users, there is a document available explaining the differentiation of the IT security standard series ISO 27000 and IEC 62443.

Planners and operators of production facilities are faced with the question of which standards are to be adhered to for the IT security concepts and, if necessary, also for auditing these facilities. Since the responsibility for IT security for operational technology (OT) often lies in different hands than for information technology (IT), there are occasionally divergent views as to which standards are to be used as a basis.

Differentiation between ISO 27001 to IEC 62443-3-3 can be found here:

- Chapter: Further Information

2.6. Device Security Assurance Center (DSAC)

ABB established an independent Device Security Assurance Center (DSAC) several years ago with certified competence to provide continuous security testing and assessments of devices. Robustness testing is performed by highly trained specialists in close collaboration with the suppliers of the test platforms. ABB proactively takes measures to improve the security of the product offering. These measures follow commonly accepted industry standards and practices and include, where technically feasible:

- Robustness testing, including fuzzing and flooding
- Vulnerability scanning for known vulnerabilities and exploits
- Security testing, including static code analysis or binary code analysis

Figure 1 shows the Cyber-Security test process at DSAC.

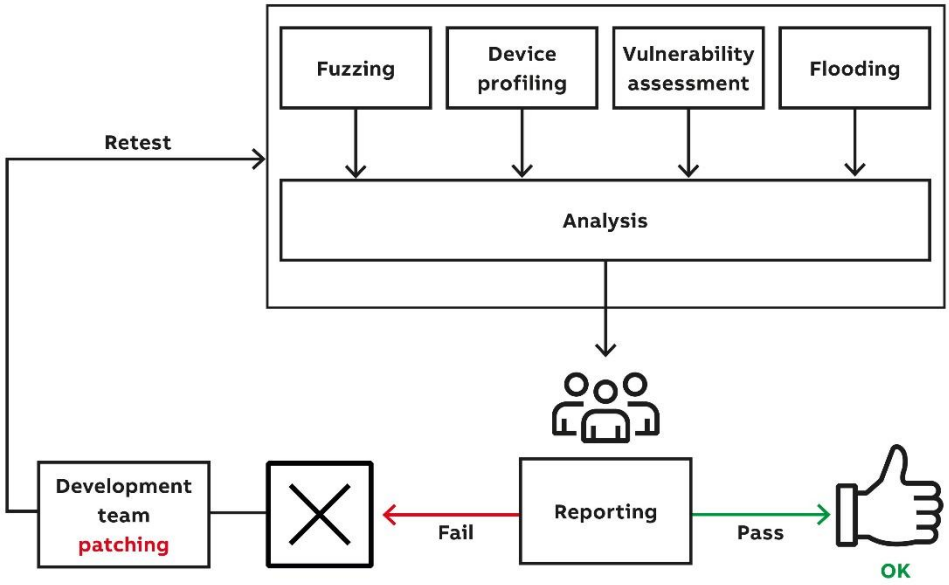

Figure 1 - Cyber security testing[4]

2.7. Achilles Testing

We are testing each firmware according to Achilles Level I and Level II. Further information's can be found in chapter: Device Security Assurance Center (DSAC).
The Achilles certificates can be found here:

- Certificate AC500 V2 and AC500-eCo V2 CPUs
- Certificate AC500 V3 and AC500-eCo V3 CPUs

2.8. Vulnerability handling[7]

ABB is committed to providing 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 our customers minimize risks associated with cyber security.

ABB provides Cyber Security alerts and notifications reporting. Interested parties can subscribe with email address to the AC500 security alerts..

Reporting a vulnerability[7]

Anyone who discovers a software vulnerability affecting an ABB product is encouraged to contact ABB directly. Alternatively they can contact any national CERT.

Vulnerability reports can be submitted directly to ABB's Cyber Security Response Team, which acts as the official ABB CERT, using the email address: cybersecurity@ch.abb.com.

ABB recommends using PGP to securely transmit sensitive data. The public PGP key for the ABB Cyber Security Response Team is available on the ABB Cyber Security portal (https://www.abb.com/cybersecurity) in the "Alerts and Notifications" section under "Report a vulnerability". It can also be accessed directly via this link: Public PGP Key for ABB Cyber Security Response Team

If someone discovers a vulnerability relating to an ABB product and does not wish to contact or interact with ABB directly, we recommend contacting ICS-CERT (https://ics-cert.us-cert.gov), any other national CERT instead.

If the reporting entity does not wish remain anonymous, ABB will acknowledge them when the vulnerability is disclosed, e.g. as part of official ABB advisories.

3. How products meet the challenges

This chapter provides basic information about the cyber security reference architecture and information sources for the AC500 PLC platform and CP600 platform

3.1. Cyber Security Reference Architecture

The cyber security reference architecture defines the security context of the AC500 PLC and CP600 platform products and enables system integration in conjunction with a defense in depth approach. Figure 2 shows the reference architecture.

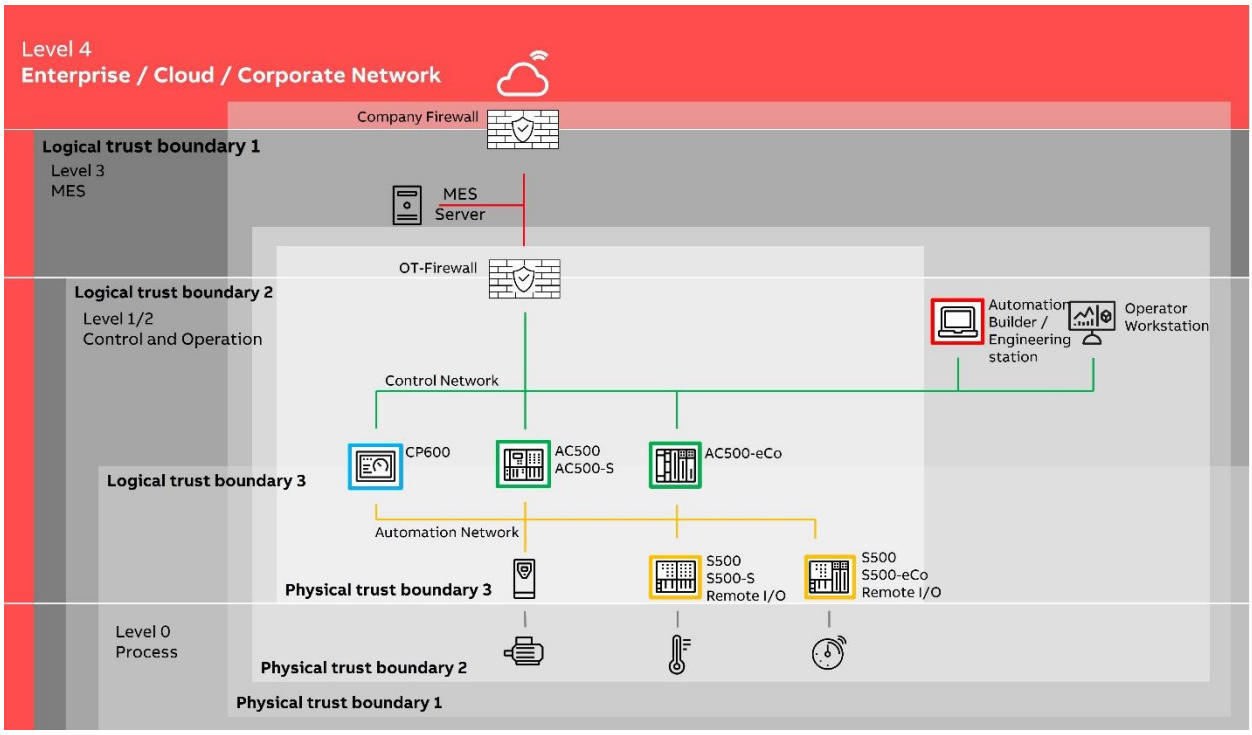

Figure 2 - Cyber Security Reference Architecture diagram for an automation system

The Cyber Security Reference Architecture includes:

- Location of the components in the network
- Isolation – physical and logicial trust boundaries as shown in Figure 2.

The reference architecture is structured into system levels, physical and logical trust boundaries

- **Logical trust boundary 1:**

  Company intranet / MES: Company firewall, centralized user authentication and authorization system

- **Physical trust boundary 1:**

  1st level physical access restrictions to all employees e.g. a fence around the factory premises in conjunction with a monitoring system and an access-monitored premises

- **Logical trust boundary 2:**

  Control network: OT firewall, user authentication and authorization systems, encrypted communication

- **Physical trust boundary 2:**

  2nd level physical access restrictions to production staff e.g. a production building with access monitoring

- **Logical trust boundary 3:**

  Process network: no trust boundary crossing

- **Physical trust boundary 3:**

  3rd level physical access restrictions to service personal e.g. a locked switch cabinet or a locked control room within the production building

The AC500 and CP600 platform products are outlined with colored frames.The colors indicate the accessibility and isolation criteria for the security requirements of the environment and the assumptions about that environment to achieve the security level for which the product was designed:

Blue: Local access via human user interface, remote access via control network, communication via control network, communication across logical trust boundaries.

Green: Remote access via control network, communication via control network, communication via process network, communication across logical trust boundaries.

Red: Local access via human user interface, communication via control network, communication across logical trust boundaries.

Amber: Communication via automation network.

3.2. Secure communication with digital certificates

A secure connection is used to protect the integrity of communication and the authenticity of the communication partners. In some cases, confidentiality is also an aspect e.g. trade secrets or other confidential information.

For the cryptographic protection, the server requires a TLS/SSL certificate to be used. A certificate essentially binds an identity to a pair of keys which are then used by the server to sign and/or encrypt the data. The following topics are relevant when considering secure communication:

Certificate Authority (CA)

A Certificate Authority is an entity which issues Digital certificates. These authorities have their own certificate for which they use their **private key** to sign the issued TLS/SSL or Digital Certificate. This certificate is known as the Root Certificate.
The CA's Root Certificate, and therefore, **public key**, is installed and **trusted** by default in browsers such as Chrome, Firefox and Edge. This is necessary to validate that the certificate of a website visited was signed by the CA's private key. Popular CA authorities include Comodo, GlobalSign, Digicert, GeoTrust, Thawte and Symantec.

- **Certificate Management in Automation Builder**
  In Automation Builder, we have the **security screen** where the user can manage the certificates on the PLC for all required purposes (log-in, boot application, protocols, …). Certificates can be generated by the AC500 and of course it is also possible to install any certificates.

  Further information about certificates handling, encryption methods etc., can be found in the application note here: AC500 V3 - ENCRYPTION AND CERTIFICATES

  In addition, we have created a video showing step by step guide how to encrypt communications: https://www.youtube.com/watch?v=w1117blquVw

- **Certificates for CP600 control panels**
  Panel Builder 600 projects work with certificates for several purposes such as the cryptographic protection of protocols or the project itself. Certificates can also be loaded to the control panels directly. Own x.509 certificates can be generated, and existing certificates can be imported for different use cases. Refer to the Panel Builder 600 Manual for further details.

3.3. Product documentation

Product documentation can be found here:

- Automation Builder online help
- AC500 V3 Hardware - Manual
- PB610 Panel Builder 600 - Manual
- Operating instructions CP600 control panels portfolio

3.4. How AC500 meets the challenges

3.4.1. Cryptographic tools and security functionalities of AC500 V3

The AC500 V3 offers all security features to integrate optimally into an automation network. In particular, the AC500 V3 supports the following security functionalities:

- Support of TLS v1.2
- Signed firmware updates and a list of SHA-256 hashed for validation of the firmware downloads from the ABB server
- Signed boot project
- Signed libraries

3.4.2. Default open Ports

As part of the ABB security concept the AC500 V3 PLC has minimal services open by default. Only those required for initial setup and programming are open prior to the download of the user application. Default open Ethernet ports of AC500 V3 and AC500-eCo V3 CPUs are:

- ABB NetConfig[1] UDP: 24576
- Communication between engineering software and PLC[2] TCP: 11740
- OPC UA server[3] TCP: 4840

Remarks:

1. The UDP port 24576 is used for initial setup of the network configuration. For example, to set the initial IP address. This port does not provide any further functionality besides that.

   The port 24576 for ABB NetConfig protocol can be disabled via PLC configuration by deleting the protocol node from configuration tree of Ethernet interfaces ETH1 and ETH2.

2. The TCP port 11740 is used for communication between the AC500 controller and the Automation Builder engineering software. This port does not provide any further functionality besides that.

3. The port 4840 for OPC UA server is closed by default as of System Firmware V3.1.0 and newer.

Besides UDP port 24576 and TCP port 11740 no other proprietary protocols are used.

3.4.3. Supported Secure protocols

Server protocols:

• FTPS	TCP: 21
• HTTPS	TCP: 443
• OPC UA	TCP: 4840
• Encrypted Communication between engineering software and PLC	TCP: 11740
• Custom TCP protocols secured by TLS	TCP: User defined
• DNP3 Outstation with SAv5.	TCP: 20000

Client protocols:

• Mqtt	TCP - Src Port: random, Dst Port: user defined
• OPC UA	TCP - Src Port: random, Dst Port: user defined
• Custom TCP protocols secured by TLS	TCP - Src Port: random, Dst Port: user defined

All the certificates for the different protocols can be handled in the Security Screen marked with this icon in the status bar or via View menu. The default ports can be changed in the settings.

FTP AND FTPS[8]

File Transfer Protocol (FTP) and File Transfer Protocol Secure (FTPS) are used for transferring files between devices. The AC500 can act as FTP server in this case.

An FTP client can open an FTP session and store and retrieve files to and from the FTP server (AC500). Focus applications are large monitoring and diagnosis networks, where e.g. thousands of plants have to independently send their data to servers and may fetch files containing updates, commands, etc.). In case of FTPS, a certificate must be installed on the PLC.

FTP Vulnerabilities:

FTP uses unencrypted data transfer and, hence, user credentials and file contents can be eavesdropped on. FTPS requires a certificate inside the PLC and should be preferred.

Using FTP for official file transfer can leave your data transmission exposed to many security attacks like:

- FTP Bounce Attack
- FTP Brute Force Attack

Measures to Reduce Risk of FTP use:

- FTP is disabled by default. Do not enable it if it is not required
- Allow only connections to known devices
- Keep the server and client software / firmware up to date

Recommendation:

- It is recommended to use secure protocols like FTPS instead of FTP if possible
- See: AC500 V3 - ENCRYPTION AND CERTIFICATES

HTTP and HTTPs

Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol Secure (HTTPS) are used to request information from a server or send information to the client.

By default, HTTP uses TCP port 80 and HTTPS uses TCP port 443.

HTTPS transmits HTTP telegrams with encryption, commonly using TLS or SSL.

The AC500 uses a webserver for the web visualization. Both protocols HTTP and HTTPS are supported. In case of HTTPS, a certificate must be installed on the PLC.

HTTP Vulnerabilities[6]:

- Broken Authentication
- Cross Site Scripting (XSS)

Measures to reduce the risk of HTTP use:

- HTTP is disabled by default. Do not enable it if it is not required
- Allow only connections to known devices
- Keep the server and client software / firmware up to date

Recommendation

- It is recommended to use secure protocols like HTTPS instead of HTTP if possible
- See: AC500 V3 - ENCRYPTION AND CERTIFICATES

OPC UA

OPC UA (Open Platform Communications Unified Architecture) is a collection of standards for communication and data exchange in the field of industrial automation. OPC UA describes both the transport of machine-to-machine data and interfaces as well as the semantics of data. The complete architecture is service-oriented.

AC500 supports TLS for OPC UA secure communication. Also needs a certificate on the PLC as well as a client certificate that also needs to be stored on the PLC.

OPC UA Vulnerabilities:

- Broken Authentication

Recommendation:

- Keep the server and client software / firmware up to date
- Use secure connection between server and client

SECURITY SCREEN

Together with Automation Builder we can activate the use of certificates for extended security. The following security features are available inside the Security Screen in Automation Builder:

Encrypted communication

When the user communicates with the controller, the server certificate of the controller is used for establishing an encrypted connection. Then the entire communication is encrypted.

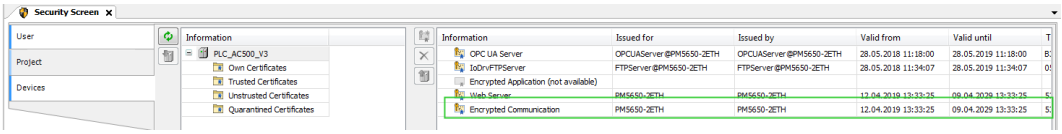

Figure 3 - Security Screen in AB

Recommendation:

- Using secure online protocol for connecting to the PLC with Automation Builder
- See: AC500 V3 - ENCRYPTION AND CERTIFICATES

3.5. How CP600 meets the challenges

3.5.1. Cryptographic tools and security functionalities of CP600

CP600 control panels offer all security features to integrate optimally into an automation network. In particular, the CP600 portfolio supports the following security functionalities:

- TLS V1.2 and 1.3
- Signed BSP (Board support package)
- Encrypted project files
- Signed projects

3.5.2. Default open Ports

Ports used for the main operations

Port		Where used
443/tcp	HTTPs	Project management, System Settings, Remote access (Remote Client, Web Browser)
990/tcp	FTPs	Project management, System Settings, Remote access (Remote Client, Web Browser)
990-991/udp		UDP broadcast (Device discovery)

3.5.3. Supported Secure protocols

Server protocols:

- FTPS — TCP: 990
- HTTPS — TCP: 443
- OPC UA — TCP: 48010

Client protocols:

- Mqtt — TCP - Src Port: random, Dst Port: user defined
- OPC UA — TCP - Src Port: random, Dst Port: user defined
- CODESYS V3 Handler — TCP - Src Port: random, Dst Port: 11740
- FTPs — TCP - Src Port: random, Dst Port: user defined

For secure communication between AC500 PLCs and CP600 HMIs, CODESYS V3 Handler is the recommended protocol. It should always be used in combination with AC500 user management and encrypted communication.

3.6. Hardening[11]

The purpose of system hardening is to eliminate as many security risks as possible. Hardening your system is an important step to protect your personal data and information. This process is intended to eliminate attacks by patching vulnerabilities and turning off inessential services. Hardening a system involves several steps to form layers of protection.

3.6.1. Commissioning phase

The following measures should be applied during the commissioning phase in order to harden the system.

- Protect the hardware from unauthorized access
- Be sure the hardware is based on a secure environment
- Disable unused software and services (network ports)
- Install firewalls
- Inhibit file sharing between programs
- Install virus and spyware protection (endpoint protection) on the PC based systems
- Use containers or virtual machines, if possible
- Create strong passwords by applying a strong password policy
- Creating and keep backups, test the restore
- Use encryption when possible
- Disable weak encryption algorithms
- Enable and use disk quotas
- Use access control
- Adjust default settings, especially passwords

3.6.2. Operation phase

The following measures should be applied during the operation phase

- Keep software up to date, especially by applying security patches
- Keep Antivirus up and running
- Keep antivirus definitions up to date
- Delete unused user accounts

3.6.3. Decommissioning phase

The following measures should be applied during the decommissioning phase

- Delete licenses
- Delete certificates
- Delete user accounts
- Delete applications and user data
- Safe disposal: If a reset origin device (reset to factory default) is not possible, it is recommended to destroy the device prior to disposal.

3.7. Defense in Depth[12]

The defense in depth approach implements multi-layer IT security measures. Each layer provides its special security measures. All security mechanisms deployed in the system must be updated regularly. It's also important to follow the system vendor's recommendations on how to configure and use these mechanisms. As a basis, the components must include security functions such as:

- Virus protection
- Firewall protection
- Strong and regularly changed passwords
- User management (Application Note – AC500 User management)
- Using VPN tunnels for connections between networks
- Physical protections
- Access control

Additional security components such as routers and switches with integrated firewalls should be considered. A defined user and rights concept managing access to the controllers and their networks is mandatory. Finally, the manufacturer of the components should be able to quickly discover weaknesses and provide patches.

3.7.1. Using Security Zones[14]

IT resources vary in the extent to which they can be trusted. A common security architecture is therefore based on a layered approach that uses zones of trust to provide increasing levels of security according to increasing security needs. Less-trusted zones contain more-trusted zones and connections between the zones are only possible through secure interconnections such as firewalls (see Figure 4). All resources in the same zone must have the same minimum level of trust. The inner layers, where communication interaction needs to flow freely between nodes, must have the highest level of trust. This is the approach described in the IEC 62443 series of standards.

Firewalls, gateways, and proxies are used to control network traffic between zones of different security levels, and to filter out any undesirable or dangerous network communication. Traffic that is allowed to pass between zones should be limited to what is necessary because each type of service call or information exchange translates into a possible route that an intruder may be able to exploit. Different types of services represent different risks. Internet access, incoming e-mail and instant messaging, for example, represent very high risks.

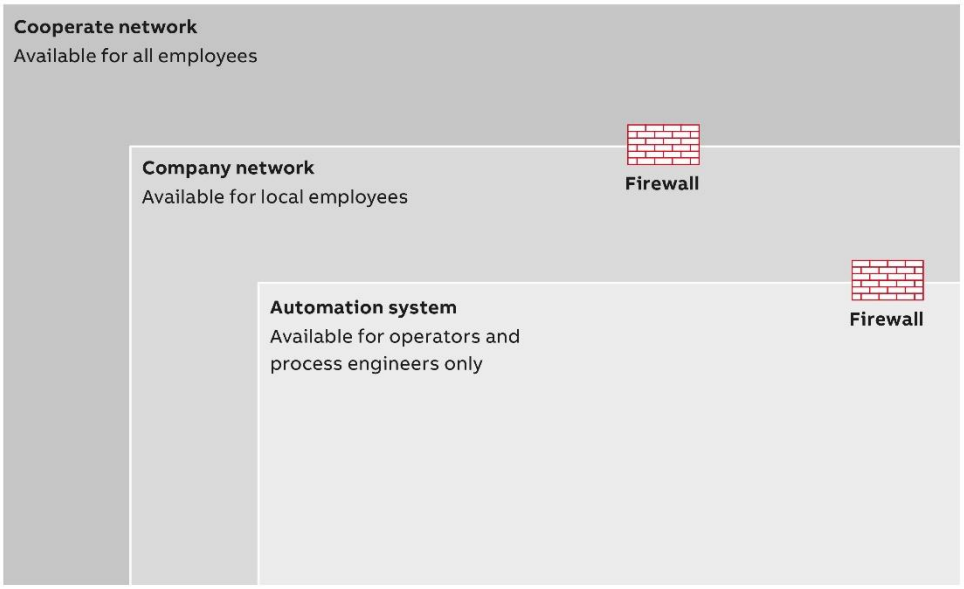

Figure 4 - Security Zones

Figure 4 shows three security zones, but the number of zones can be more or fewer as three. Using multiple zones enables the access between zones of different trust levels to be controlled, protecting a trusted resource from attack by a less trusted one.

High-security zones should be kept small and independent. They need to be physically protected, i.e. physical access to computers, network equipment and network cables must be limited by physical means to authorized people only. A high-security zone should obviously not depend on resources in a less secure zone for its security. Therefore, it should form its own domain that is administered from the inside and not depend on e.g. a domain controller in a less secure network.

Even if a network zone is regarded as trusted, an attack is still possible, either from a user or compromised resource inside the trusted zone, or from an outside user or resource that succeeds in penetrating the secure interconnection. Therefore, trust also depends on the measures taken to detect and prevent the compromise of resources and violations of the security policy.

3.7.2. Using protected environment

The devices must be located in a protected environment to avoid accidental or intended access to the controller or the application. Such a protected environment can be:

- Locked control cabinets without connection from outside
- No direct internet connection
- Use firewalls and VPN to separate different networks
- Separate different production areas with different access controls

To increase security, physical access protection measures such as fences, Turnstiles, cameras or card readers can be added. In addition, we must follow some rules for the protected environment:

- Keep the trusted network as small as possible and independent from other networks.
- Protect the cross-communication of controllers and the communication between controllers and field devices via standard communication protocols (fieldbus systems) using appropriate measures.
- Protect such networks from unauthorized physical access.

- Use fieldbus systems only in protected environments. They are not protected by additional measures, such as encryption. Open physical or data access to fieldbus systems and their components is a serious security risk.
- Physically protect all equipment, i.e. ensure that physical access to computers, network equipment and cables, controllers, I/O systems, power supplies, etc., is limited to authorized personnel.
- When connecting a trusted network zone to outer networks, make sure that all connections are through properly configured secure interconnections only, such as a firewall or a system of firewalls, which is configured for “deny by default”, i.e. blocks everything except traffic that is explicitly needed to fulfill operational requirements.
- Allow only authorized users to log on to the system, and enforce strong passwords that are changed regularly.
- Continuously maintain the definitions of authorized users, user groups, and access rights, to properly reflect the current authorities and responsibilities of all individuals at all times. Users should not have more privileges than they need to do their job.
- Do not use the automation system for e-mail, instant messaging, or Internet browsing. Use separate computers and networks for these functions if they are needed.
- Do not allow installation of any unauthorized software in the system.
- Restrict temporary connection of portable computers, USB memory sticks and other removable data carriers. Computers that can be physically accessed by regular users should have ports for removable data carriers disabled or locked.
- If portable computers need to be connected, e.g. for service or maintenance purposes, they should be carefully scanned for viruses immediately before connection.
- All CDs, DVDs, USB memory sticks and other removable data carriers as well as any files containing software or software updates, should be scanned for viruses before being introduced to the trusted zone.
- Continuously monitor the system for intrusion attempts.
- Define and maintain plans for incident response, including how to recover from potential disasters.
- Regularly review the organization as well as technical systems and installations with respect to compliance with security policies, procedures and practices.
- Use user management in the control panel project to prevent unauthorized operations via the touchscreen.

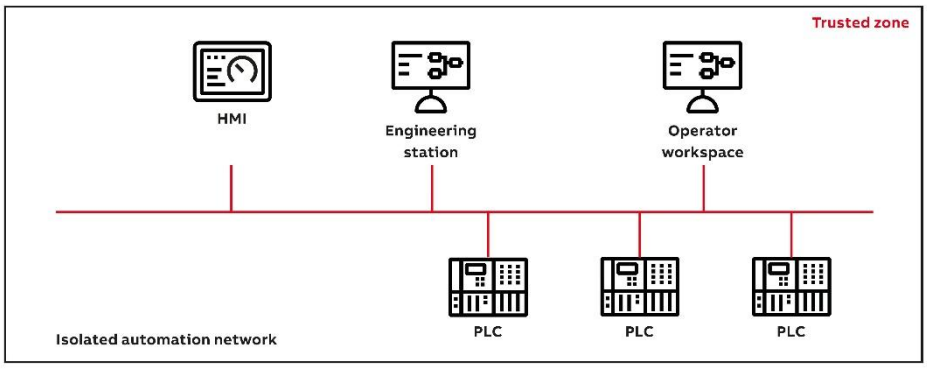

Figure 5 - Isolated Automation System

Figure 5 shows what a protected, local, isolated automation network could look like. This network is not connected to any external network. Security primarily involves physically protecting the automation system and preventing unauthorized users from accessing it, as well as preventing them from connecting or installing unauthorized hardware and software.

Servers and workplaces not directly involved controlling l and supervising of the process should be connected to a subnet separated from the automation system network by a router/firewall, if possible. This enables better control the network load limits access to certain servers on the automation system network. Please note that servers and workplaces on this subnet are part of the trusted zone and therefore require the same security precautions as the nodes on the automation system network.

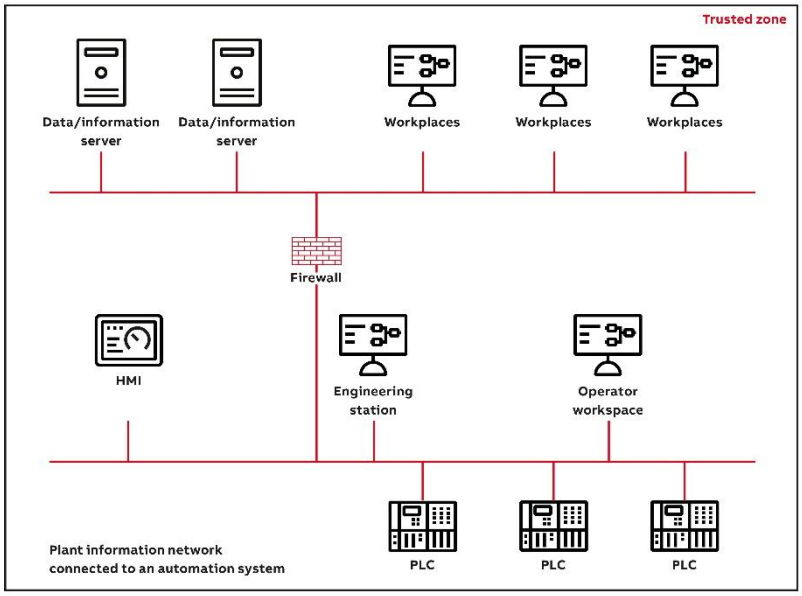

Figure 6 - Plant information network connected to an automation system

For the purposes of process control security, a general-purpose information system (IS) network should not be considered a trusted network, not the least since such networks are normally further connected to the Internet or other external networks. The IS network is therefore a different lower-security zone, and it should be separated from the automation system by means of a firewall. The IS and automation system networks should form separate domains.

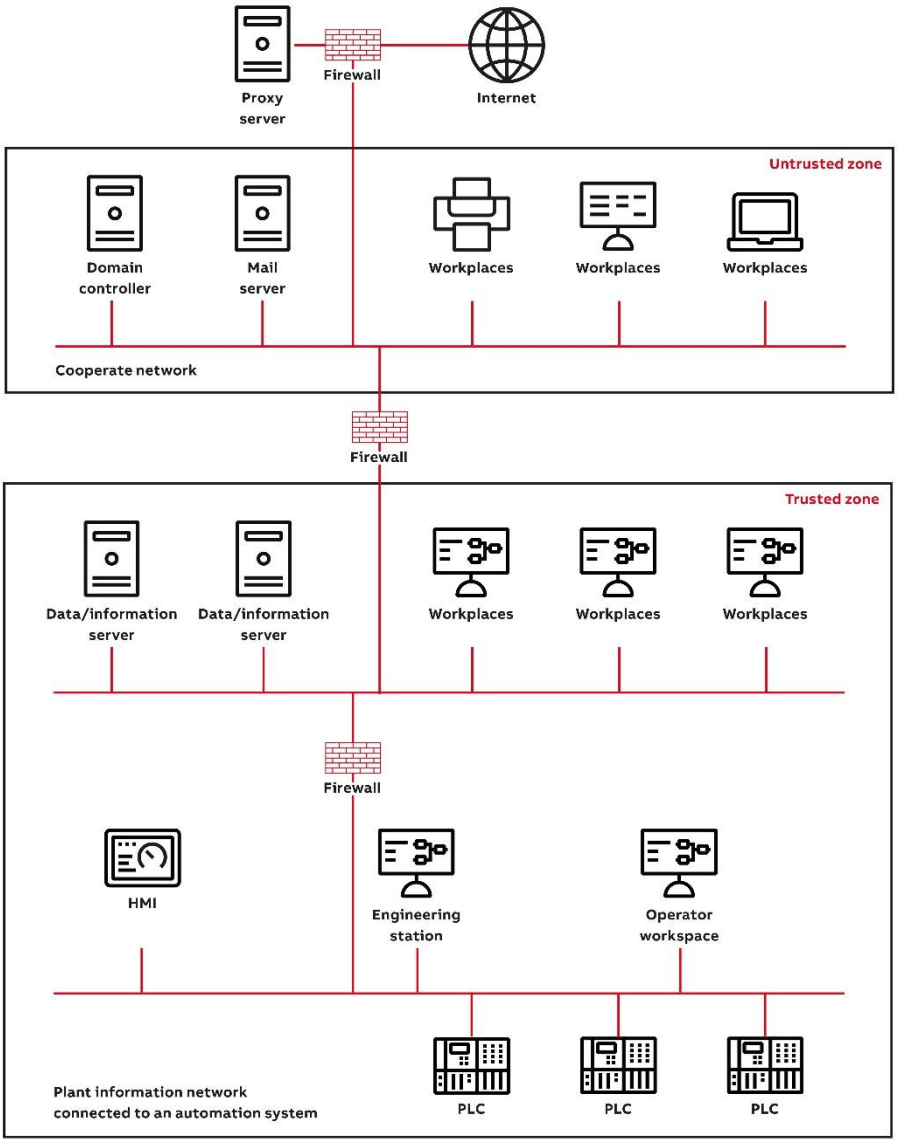

Figure 7 - Automation system and IS network

3.8. Whitelisting[13]

The primary purpose of whitelisting is to protect computers and networks from harmful applications. The whitelist is simply a list of applications that have been granted permission to run by the user or administrator. When an application attempts to start, the whitelisting algorithm automatically checks against this list. If the application is on the list, it is allowed to run.

An integrity check, such as hash value check, usually verifies that the application is authorized and not a malicious program operating under the same name.

If possible, whitelisting should be preferred over blacklisting. A whitelist gives system access to administrator-approved programs, and IP and email addresses. Anything not on the list is blocked.

4. Cyber Incident Checklist

Every business should have a security checklist. This checklist contains useful tips and questions to ask yourself before you commissioning your application.

The top points of a security checklist for protecting yourself from known cyber threats are as follows:

- **Keep your software updated**

  Daily check if a new version is available

- **Keep your firmware updated**

  Daily check if a new version is available

- **Use strong password policy**

  Use strong and complex passwords of at least eight characters with a combination of uppercase and lowercase letters, numbers and special characters

- **Use automatic screen lock**

  When a computer or mobile device has been idle for a few minutes, it should be set to automatically lock the screen.

- **Storing data**

  Check where you are saving your data. Be sure you also check your cell phone, USB devices, SD cards, Cloud memory and backup systems.

- **Secure devices**

  Any device that contains company and client data needs to be physically or digitally secured. On-premise file servers need to be in a locked room/cage and the office should have a security system. Mobile devices need to be locked when not in use and any data drives have to be encrypted.

- **Educate employees**

  Security education is very important. Ensure that all employees are trained in cybersecurity including methods such as phishing and pharming, as well as threats such as ransomware and social engineering, which are used by hackers access the a user's computer.
  Also, provide training on the coprrect way to handle emails. Never click on a link in an email if you have any doubts about the sender.

5. Support

5.1. Supporting tools

To support customers effectively and manage security features, ABB provides a number of application examples and technical notes. These resources are available on our official website:

https://new.abb.com/plc/application-examples

Starting with Automation Builder V2.8.0, a new feature allows users to generate a comprehensive security report. This tool facilitates the documentation and review of security configurations. Detailed instructions can be found in the online help portal:

https://help.plc.abb.com/?topic=cyber_security_report_in_ab

Furthermore, starting with Automation Builder V2.8.1, a Syslog client feature was introduced. This feature enables the transmission of all audit events to a specific server, thus improving traceability and compliance. Documentation for this feature is currently being developed. The shared log is explained here:

https://help.plc.abb.com/?navbar=false&q=log&sidebar=true&topic=cpu_log

5.2. Further Information

The most raised questions regarding AC500 Cyber Security are listed here:

- FAQs

Differentiation between ISO 27001 to IEC 62443 can be found here:

- English version
- German version

IEC 62443 from the planner's and operator's point of view

- English version
- German version

Additional information can be found in the Automation Builder documentation:

- AC500 V2 Manual
- AC500 V3 Manual or online help

5.3. Contact

For additional information and support, please contact your local ABB service organization.

- https://access.motion.abb.com/contact/contact

Information about ABB's cyber security program and capabilities can be found here:

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

ABB Cyber Security - Alerts & Notifications can be found here:

- Alerts and Notifications

6. Glossary

Term	Description
AB	Automation Builder
Broken Authentication[6]	Broken authentication and session management encompass several security issues, all of them having to do with maintaining the identity of a user. If authentication credentials and session identifiers are not protected at all times, an attacker can hijack an active session and assume the identity of a user.
BSP	Board support package
CA	Certification Authority
Cross Site Scripting (XSS)	Cross-site scripting (XSS) targets an application's users by injecting code, usually a client-side script such as JavaScript, into a web application's output. The concept of XSS is to manipulate client-side scripts of a web application to execute in the manner desired by the attacker. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface websites, or redirect the user to malicious sites.
DSAC	Device Security Assurance Center
FTP Bounce Attack	Generally, a file transfer happens when the source FTP server sends the data to the client which transmits the data to the destination FTP server. When there's a slow network connection, people often resort to using a proxy FTP which makes the client instruct the data transmission directly between two FTP servers. A hacker can take advantage of this type of file transfer and use a PORT command to request access to ports by posing as a middle man for the file transfer request; they then execute port scans on hosts discreetly and gain access data transmitted over the network.
FTP Brute Force Attack	An attacker can carry out a brute force attack to guess the FTP server password by implementing a means to repeatedly try different password combinations until they can succeed in the break-in. A weak password and repeated use of the same password for multiple FTP servers can also help the hacker gain quick access. Once the password is guessed, your data is exposed.
ICS	Industrial Control Systems
IT	Information Technology
LAN	Local Area Network
MCSR	Minimum Cyber Security Requirements
OT	Operating Technology
Packet Capture (Sniffing)	Because the data transfer via FTP is in clear text, any sensitive information such as usernames, passwords can be easily read via network packet capture techniques such as packet sniffing. A packet sniffer is just a piece of computer program which can capture transmitted data packets and decode the packet's raw data exposing data contained in the various fields of the packet.
PGP	Pretty Good Privacy. It's a public key block.

Port Stealing	When operating systems assign dynamic port numbers in a particular order or pattern, an attacker easily decodes the pattern and identifies the next port number which will be used. By illegally gaining access to a port number, the legitimate client trying to access the file will be denied access, and the hacker can steal files or even insert a forged file or malicious file into the data stream which will be accessed by other legitimate users in the organization.
Security Misconfiguration	Security misconfiguration often using defaults that were not changed like keys and passwords.
Spoof Attack	When we restrict access to FTP servers based on the network address, it is possible for a cyber-criminal to use an external computer and assume the host address of a computer on the enterprise network and download files during data transfer.
SQL injection	SQL injection is a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content. If successful, this allows the attacker to create, read, update, alter, or delete data stored in the back-end database. SQL injection is one of the most prevalent types of web application security vulnerabilities.
SSL[9]	SSL (Secure Sockets Layer) is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browsers remain private and ensure their integrity. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers.
TLS[10]	TLS (Transport Layer Security) is a protocol that provides privacy and data integrity between two communicating applications. It's the most widely deployed security protocol used today, and it is used for Web browsers and other applications that require data to be securely exchanged over a network.
SAv5	Secure Authentication Version 5.

7. References

Nr.	Link
1.	https://search.abb.com/library/Download.aspx?DocumentID=8VZZ000367T0027&LanguageCode=en&DocumentPartId=&Action=Launch
2.	http://1https//www.securityweek.com/ibm-reports-significant-increase-ics-attacks
3.	https://mcuoneclipse.com/2017/04/14/enable-secure-communication-with-tls-and-the-mosquitto-broker/
4.	https://library.e.abb.com/public/03f77d8934134c72865f88cc61b59798/ABB_Device_Security_Assurance_Center(DSAC)_9AKK107680A9866.pdf
6.	https://www.quora.com/What-are-the-security-vulnerabilities-in-HTTP
7.	http://www.abb.com/cybersecurity
8.	https://thehackernews.com/2013/12/security-risks-of-ftp-and-benefits-of.html
9.	http://info.ssl.com/article.aspx?id=10241
10.	https://searchsecurity.techtarget.com/definition/Transport-Layer-Security-TLS
11.	https://en.wikipedia.org/wiki/Hardening_(computing)
12.	https://customers.codesys.com/fileadmin/data/customers/security/CODESYS-Security-Whitepaper.pdf
13.	https://www.computerweekly.com/de/definition/Application-Whitelisting
14.	https://library.e.abb.com/public/b1f29a78bc9979d7c12577ec00177633/3BSE032547_B_en_Security_for_Industrial_Automation_and_Control_Systems.pdf
15.	https://www.abb.com/global/en/company/about/cybersecurity/nis-2-at-abb

8. Document history

Rev.	Description of version / changes	Date
10	• New title picture • Replaces all pictures, following ABB style • Added chapter: Default open Ports • Updated chapter: Supported Secure protocols • Removed certificates handling and linked to application note • Added Document history • Footer changed	15.02.2024
11	• Small changes in chapter: Default open Ports	16.04.2024
12	• Added Achilles Level II certificate for AC500 V3 PLC in chapter: Achilles Testing	27.06.2024
13	• Added links to application notes • Updated broken links • Formatting of hyperlinks • Set new contact in chapter: Contact • Added DNP3 port • Add Capabilities for IEC62443-4-2	09.09.2024
14	• Updated chapter: Supported Secure protocols - DNP3 • Added Sav5 to glossary	10.10.2024
15	• Added link to online help • Added signed libraries and linked to online help • Added video how to encrypt communication • Added list of SHA-256 hashes for FW versions • Added NIS2 • Modified ISO27001 • Added CP600 specific parts in how the product meets the challenges • Added supporting tools • Changed order of chapters	15.01.2026
16	• Added chapter: Cyber Security Reference Architecture • Removed: Best Practice for secure network chapter • Fixed formatting issues	17.03.2026

ABB AG

Contact:
https://access.motion.abb.com/contact/contact

Homepage:
www.abb.com/plc