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.

Cyber Security has become of key importance for ABB customers and ABB alike. In order to help protect ABB customers as well as our brand, cyber security must be an important aspect in our products, systems, projects and service deliveries.

The development of Industrial **C**ontrol **S**ystems **(ICS)** over the past two decades has changed the face of many industries. **O**perational **T**echnology **(OT)** – largely industrial equipment – has become increasingly connected, and the integration of **I**nformation **T**echnology **(IT)** components allows such devices to leverage software that drives data collection and analysis, resulting in enhanced performance and ultimately "smarter" machines. The AC500 product family comprises devices that control and monitor processes or events in a physical world. These common systems are used in industries such machine building, infrastructure and others.

With these benefits came vulnerabilities, including the possibility of malicious actors gaining access to critical assets through networks. The growing recognition of cyber security threats to critical infrastructure (e.g. energy, water, transportation) has brought the topic into the spotlight. Regulatory requirements for these industries have increased as well. Standards and policies have been created in an attempt to address the rapid technological changes; however, it is still challenging for companies to implement the necessary processes and keep personnel up to date and trained. Meanwhile, the cyber threat landscape continues to diversify. According to IBM, the number of attacks aimed at ICS increased by 110% from 2015 to 2016. To add to this, leveraging third-party vendors and new cloud-based services result in additional areas of risk previously non-existent in ICS.

Designing products in a way to be protected against cyber-attacks only became a topic of concern about a decade ago, and the prevailing sense at that time was that isolation ("air gap") and limited availability of technical knowledge ("security by obscurity") protected ICS products. However, with often changing equipment and life cycles counted in decades, it will take time for secure components to become the norm.

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

2. Applicability (The challenges)[1]

2.1. Regulatory requirements

In an effort to address cyber security risks, the number of regulations and standards that have been created by governments, industry groups and private organizations has grown considerably over the past 10 years. Organizations must go through the effort of understanding the regulatory environment, determine which regulatory requirements are applicable to them, and then continuously monitor for updates and changes to regulation to confirm compliance with the latest versions. Additionally, there is a very real threat that even when an organization attempts to faithfully comply, a lapse in proper execution can expose them to potential fines.

Having to meet regulatory requirements, the endless focus on compliance and the reporting and documentation that this entails, can be both daunting and taxing. Nevertheless, this is necessary because compliance very often is a prerequisite for doing business with customers. It is a way to show that the minimum cyber security requirements have been met.

In reality, compliance is a byproduct of security. Organizations need to look at security from a holistic standpoint, not a 'check-the-box' or bare-minimum compliance standpoint.

Recommendations on how to approach security more comprehensively follow in the sections below.

2.2. Workforce shortages

The three pillars of cyber security are people, processes, and technology. While many organizations' policies focus on the latter two factors, it should be noted that people are just as critical to maintaining a robust security posture.

The tremendous changes in technology are now resulting in increased demand for new skills and skills combinations; the current demand for cyber professionals is not being met.

Recommendations: Many companies address this shortfall by building collaborative teams drawn from both IT and OT staff within the organization. Other organizations turn to third party providers to deliver IT/OT expertise that is shared among multiple customers through managed services. Automation of routine security maintenance tasks and reporting can significantly reduce this burden as well.

A positive effect is that retraining programs and a greater interest in the cyber security field from a professional education perspective are becoming increasingly common.

Some of the major cyber security training programs and certifications are:

- **SANS Institute** – largest provider of cyber security training, focus on preparing people for cyber security certifications and other widely recognized programs in the industry
- **CISSP** – Certified Information System Security Professional, considered a rite of passage for CISO (Chief Information Security Officer) professionals
- **GICSP** – Global Industrial Cyber Security Professional, the certification to CISSP recognized within industry

2.3. Life cycle of products

As mentioned previously, in the past ICS systems were not designed with cyber security as a first priority. While organizations may have more opportunities to implement cyber security standards in new products and systems, it can be more difficult to improve older ICS. This difficulty notwithstanding, organizations are still expected to address the cyber security needs of these legacy systems, which are likely to have far fewer support options.

This means that remediation needs for older ICS are at times unknown to the organization, and when known can be challenging and costly. In addition, many product life cycles are counted in decades rather than years, and it is not always straightforward to find capital to replace or upgrade products quickly.

Recommendations: Together with ICS system providers, organizations should evaluate their existing operations base and prioritize remediation. A risk assessment will highlight what is worth fixing immediately. Organizations can prioritize and still greatly impact their risk posture.

Moving forward, organizations need to ensure that their programs and systems are secure by design and secure by default so that they do not have the same challenges in the next generation of products.

3. Requirements (Understanding the product design)

3.1. 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 is a confirmation that CoE PLC Products develops Secure-by-design products.

Security for industrial automation and control systems - Part 4-1: **Secure product development lifecycle requirement** certificate can be found here:

- Certificate

This 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

3.2. 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

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

3.3. ISO 27001 - Information security management systems

We are pleased to announce that Bureau Veritas has certificated site ABB AG in Heidelberg accordance with the ISO 27001 standard.

The certificate 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.

The certificate can be found here:

- Certificate

The content includes:

- 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

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

In addition to this certificate, 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.

The whitepaper for differentiate between ISO 27000 and IEC62443 can be found here:

Chapter: Further Information

3.5. Device Security Assurance Center (DSAC)

ABB established an independent Device Security Assurance Center (DSAC) already several years ago with certified competence to provide continuous protocol-stack robustness and vulnerability 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 quality of the product. 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.

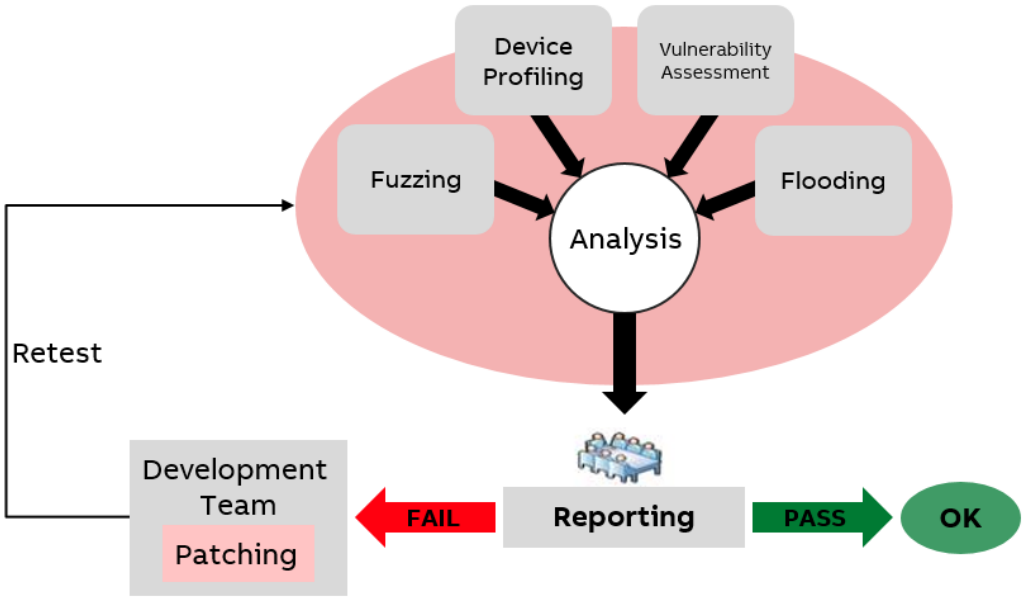

Figure 1 - Cyber security robustness testing[4]

3.6. Handling of digital certificates

A secure connection can be used to encrypt our data and protect it from being exposed to third parties.

In order for the encryption to occur, 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 encrypt and/or sign the data.

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 own certificates.

Asymmetric Encryption[5]
With the asymmetric encryption, the user has a pair of mathematically connected keys: a shared green and a private red key. The red key is kept private and is not disclosed and distributed. The green key is public: everyone can have it. Everyone can encrypt a message with the green public key, but only the keeper of the red private key is able to decrypt it:
The public and private keys form a pair. They are different, but mathematically related. This way, only the private key is able to decrypt a message encrypted with the public key.

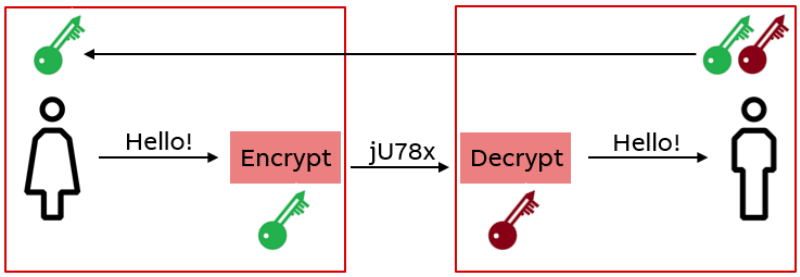

Figure 2 - Asymmetric Encryption with public and private key

Certificates[5]

Certificates are a way to establish trust and ensure that the public key is authentic and authorized.

This is where “certificates” come into play. Certificates are a proof, provided by a “Certification Authority” (CA) which testify that a key pair belongs to a specific person or device.

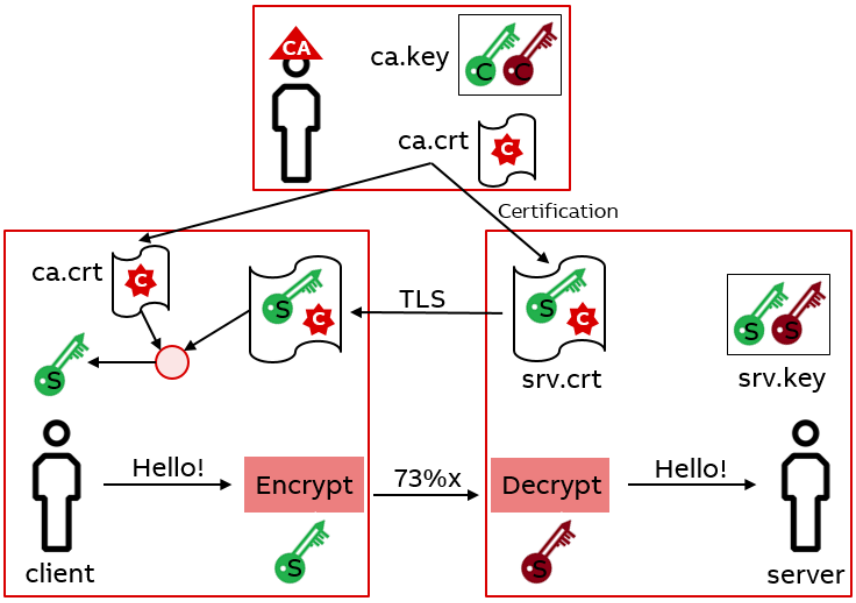

Figure 3 - simplified TLS handshake with certificates and keys[3]

3.7. Product documentation

Product documentation can be found here:

- Automation Builder
- AC500 V3 Hardware - Manual
- PB610 Panel Builder 600 - Manual
- Control Panels CP600-Pro - Operating Instructions

3.8. 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. Everyone who is interested can subscribe with their email address.

Applicability of published vulnerabilities to customer's cyber assets

It is not always a given that organizations have a full inventory or visibility of all the components across their operational enterprise, or in their ICS or those of third-party service providers. This can have a negative effect in the case of a vulnerability, as an organization tries to understand the impact on their assets and react accordingly. Where no cyber asset management system is in place, manual effort is required, resulting in increased costs and lengthy reaction times.

IT IS A CASE OF: "YOU CAN'T MEASURE WHAT YOU DON'T KNOW"

(Quote by: Peter Drucker)

Recommendations: When installing new equipment or systems, organizations should also install programs that compile a report of their asset inventory (i.e. number of servers, HMIs, etc.). Also, firewalls should be installed to protect the overall system. If you are not familiar with Cyber Security standards, you should request support from specialists.

Reporting a vulnerability[7]

Anyone discovering a software vulnerability affecting an ABB solution is encouraged to contact ABB directly, or, alternatively, any national CERT or other coordinating organization.

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 the use of PGP to securely transmit any sensitive data. The public PGP key for ABB's Cyber Security Response Team can be found on the ABB Cyber Security portal (http://www.abb.com/cybersecurity) under the sections "Alerts and Notifications" and then "Report a vulnerability" or directly by following this link: Public PGP Key for ABB Cyber Security Response Team

In case that someone discovering a vulnerability relating to an ABB product does not wish to directly contact or interact with ABB, we recommend contacting ICS-CERT (https://ics-cert.us-cert.gov), any other national CERT or other coordinating organization.

If the reporting entity does not wish to stay anonymous, ABB will acknowledge the reporting entity with the discovery of the vulnerability, e.g. as part of official ABB advisories issued based on the reported vulnerability.

4. How the products meet the challenges

4.1. Achilles Testing

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

- Certificate AC500 V2 and AC500-eCo V2 CPUs
- Certificate AC500 V3 and AC500-eCo V3 CPUs is coming soon

4.2. 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
- Signed boot project

4.3. Secure protocols

The AC500 V3 supports the following secure server protocols:

- FTPS (Default Port: 21)
- HTTPS (Default Port: 443)
- OPC UA (Default Port: 4840)
- Encrypted Communication between engineering software and PLC (Default Port: 11740)
- Custom TCP protocols secured by TLS (Default Port: User defined)

The AC500 V3 supports the following secure client protocols:

- Mqtt (Default Port: 8443)
- Custom TCP protocols secured by TLS (Default 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

FTP Reduce Risk:

- 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

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)

HTTP Reduce Risk:

- 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

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 and 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.

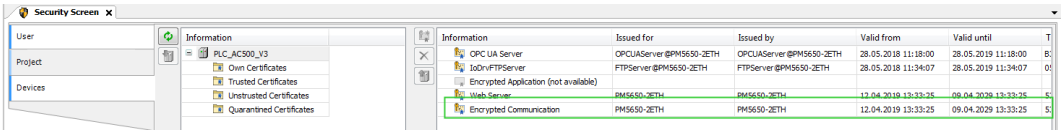

Figure 4 - Security Screen in AB

Recommendation:

- Using secure online protocol for connecting to the PLC with Automation Builder

4.4. Best Practices for secure networks

Implementing the right level of security always requires case by case considerations and decisions. This chapter provides some examples of secure networks for the related purposes. These examples must not be copied without further evaluation. To secure your network, IT security specialists should always be involved in the project.

The international standard **IEC 62443-3-1** “Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems” provides a current assessment of various cybersecurity tools, mitigation countermeasures and technologies.

Example 1: Connection of secured network

Connection of the whole AC500 network to the cloud using a separate gateway. Enhanced security is provided through additional firewall and/or VPN.

Depending on the application some additional ports must be opened to access different services. Please check the online help in Automation Builder for further information’s.

Security level advanced

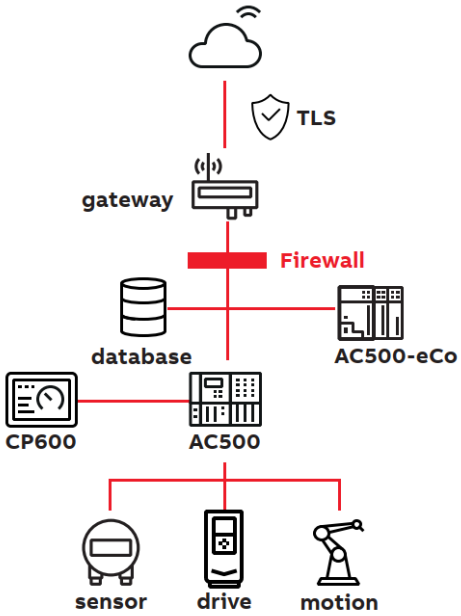

Figure 5 - Security level

Benefits:
- Advanced level of security
- Easy integration of many edge-devices

Use Case:
Large systems with many devices which need higher protection.

4.5. 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 intends to eliminate attacks by patching vulnerabilities and turning off inessential services. Hardening a system involves several steps to form layers of protection.

4.5.1. Commissioning phase

- Protect the hardware from unauthorized access
- Be sure the hardware is based on a secure environment
- Disabling unused software and services (network ports)
- Installing firewalls
- Disallowing file sharing among programs
- Installing virus and spyware protection
- Using containers or virtual machines
- Creating strong passwords by applying a strong password policy
- Creating and keeping backups
- Using encryption when possible
- Disabling weak encryption algorithms
- Separation of data and programs
- Enabling and using disk quotas
- Strong logical access control
- Adjusting default settings, especially passwords

4.5.2. Operation phase

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

4.5.3. Decommissioning phase

- Deleting licenses
- Deleting certificates
- Deleting user accounts
- Deleting applications and user data
- Safe disposal

4.6. Defense in Depth[12]

The defense in depth approach implements multi-layer IT security measures. Each layer provides its special security measures. All deployed security mechanisms 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
- Using VPN tunnels for connections between networks

Additional security components such as routers and switches with integrated firewalls should be available. 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.

4.6.1. 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 6). 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 material. Traffic that is allowed to pass between zones should be limited to what is absolutely 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.

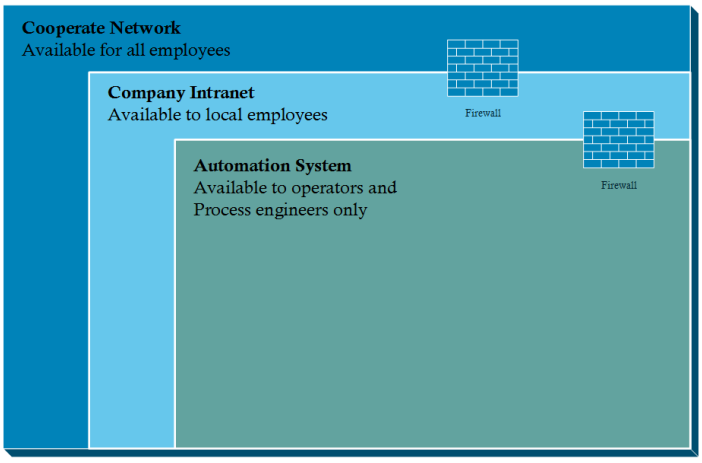

Figure 6 - Security Zones

The figure above shows three security zones, but the number of zones does not have to be as many or as few as three. The use of multiple zones allows access between zones of different trust levels to be controlled to protect 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 persons 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: by a user or compromised resource that is inside the trusted zone, or by an outside user or resource that succeeds to penetrate the secure interconnection. Trust therefore depends also upon the types of measures taken to detect and prevent compromise of resources and violation of the security policy.

4.6.2. Using protected environment

The controller must be located in a protected environment in order 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 persons

- 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 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
- 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, and files with software or software updates, should also be checked for viruses before being introduced into 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

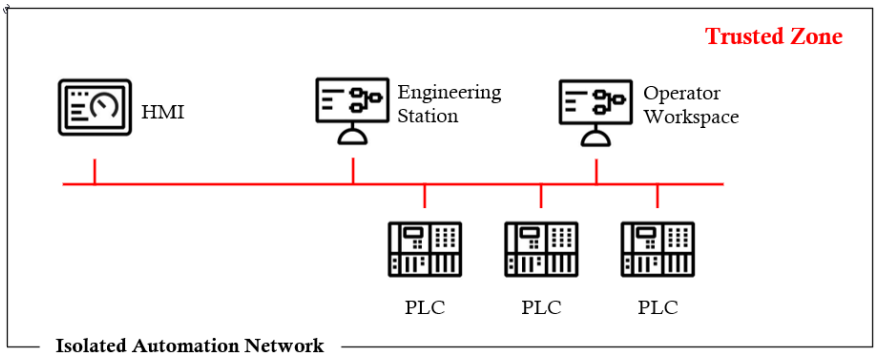

Figure 7 - Isolated Automation System

A protected local control cabinet could look like in the picture below. This network is not connected to any external network. Security is primarily a matter of physically protecting the automation system and preventing unauthorized users from accessing the system and from connecting or installing unauthorized hardware and software.

Servers and workplaces that are not directly involved in the control and supervision of the process should preferably be connected to a subnet that is separated from the automation system network by means of a router/firewall. This makes it possible to better control the network load and to limit access to certain servers on the automation system network. Note that servers and workplaces on this subnet are part of the trusted zone and thus need to be subject to the same security precautions as the nodes on the automation system network.

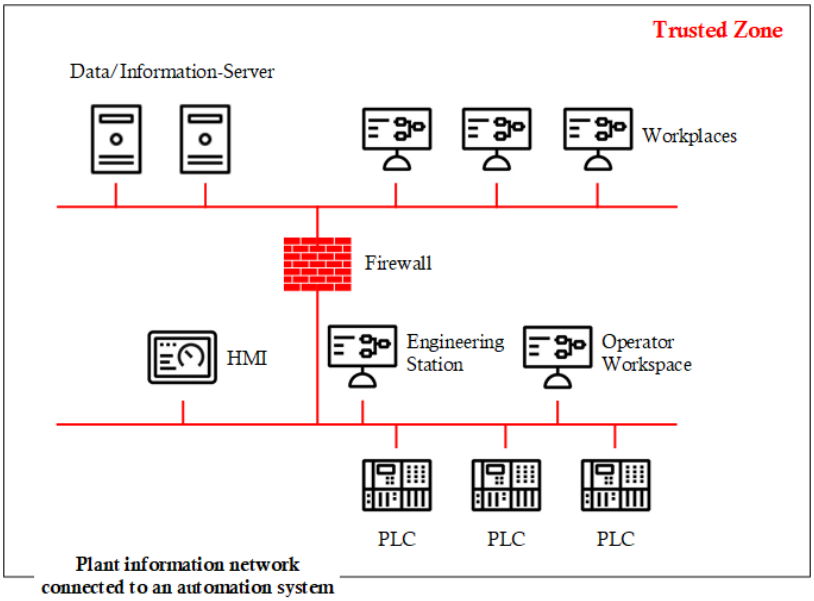

Figure 8 - Plant information network connected to an automation system

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.

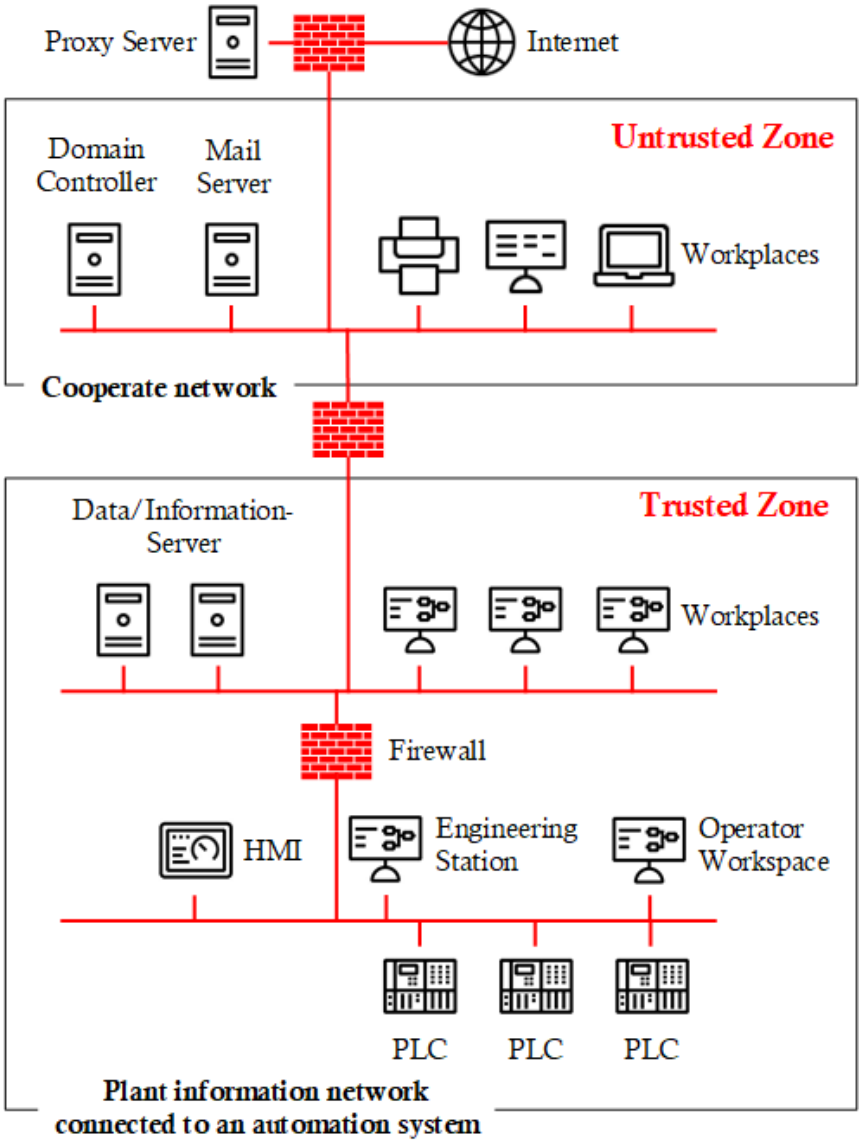

Figure 9 - Automation system and IS network

4.7. Whitelisting[13]

The purpose of whitelisting is primarily to protect the computer and network from harmful applications. The whitelist is a simple list of applications that have been given permission to execute by the user or administrator. When an application attempts to start, it will automatically check against this list. If the application is listed there, the execution is allowed.

An integrity check, such as hash values, usually checks whether it is actually the authorized application and not a malicious program that operates under the same name.

If it is possible Whitelisting should be preferred over Blacklisting. A whitelist only giving administrator-approved programs, and IP and email addresses, system access. Whatever is not on the list is blocked.

5. Cyber Incident Checklist

Every business should have a security checklist. This list contains tips and questions you should ask yourself before you commission your application.

The current top Points of a Security Checklist to protect yourself from known cyber threats are:

- **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. Be sure that all employees are trained in cyber security attacking methods such as phishing and pharming, as well as threats including ransomware and social engineering used by hackers to get access to a user's computer.
  Also train your employees regarding the right way to handle emails. Don't click on a link inside an email if you have a bad feeling about this mail's sender.

6. Support

6.1. Further Information

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

- FAQs

In addition to this document, we have published Differentiation ISO 27001 to IEC 62443

- English version
- German version

Some additional information can be found in the Automation Builder documentation:

- AC500 V2 Manual
- AC500 V3 Manual

6.2. Contact

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

For contact information, please write an email to:

- plc.support@de.abb.com

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

- ABB Cyber Security

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

- Alerts and Notifications

7. 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.
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.

8. 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/d005b0262c9b4db8b6b2c2580eb0d3ad/Cyber%20robustness%20testing%20flyer%20final.pdf
5.	https://mcuoneclipse.com/2017/04/14/introduction-to-security-and-tls-transport-security-layer/
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

ABB AG
Eppelheimer Straße 82
69123 Heidelberg, Germany
Phone: +49 62 21 701 1444
Fax : +49 62 21 701 1382
Mail: plc.support@de.abb.com
www.abb.com/plc