WHITE PAPER

Cyber Security in the AC500 PLC family

Approach Cyber Security with Confidence
Table of contents

1 Objective / Introduction ................................................................. 3
2 Applicability (The challenges) ....................................................... 4
3 Requirements (Understanding the product design) .......................... 6
   3.1 Secure Development lifecycle (SDL) ........................................... 6
   3.2 Device Security Assurance Center (DSAC) ................................. 6
   3.3 Handling of digital certificates .................................................... 7
   3.4 Product documentation .............................................................. 9
   3.5 Vulnerability handling ............................................................... 10
4 How the products meets the challenges ......................................... 11
   4.1 Cryptographic tools and security functionalities of AC500 V3 ... 11
   4.2 Best Practices for secure networks ............................................. 16
5 Cyber Incident Checklist ............................................................... 18
6 Support ......................................................................................... 19
   6.1 Contact ...................................................................................... 19
7 Glossary ....................................................................................... 20
8 References ................................................................................... 22
1 Objective / Introduction

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 Control Systems (ICS) over the past two decades has changed the face of many industries. Operational Technology (OT) – largely industrial equipment – has become increasingly connected, and the integration of Information Technology (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 their 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)  

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.

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

**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 Secure Development lifecycle (SDL)

ABB will establish, document, and implement initiatives in line with commonly accepted industry standards and practices to build security into the software development process. Such initiatives shall incorporate security into all phases of the development lifecycle, e.g., training, requirement, design, implementation, verification, release, and response.

A preparation for IEC 62443 is currently planned for the near future.

3.2 Device Security Assurance Center (DSAC)

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.

![Cyber security robustness testing diagram]

*Cyber security robustness testing*
3.3 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

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 are mathematically related. This way, only the private key is able to decrypt a message encrypted with the public key.

Certificates

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.
3.4 Product documentation

Product documentation can be found here:

- Automation Builder
- AC500 Hardware
- CP600 Software
- CP600 Hardware
3.5 Vulnerability handling

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

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 meets the challenges

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 v1.0/1.1/1.2
- Signed firmware
- Signed boot project

The AC500 V3 supports the following secure protocols:

- FTPS
- HTTPS
- OPC UA
- Encrypted Communication between engineering software and PLC
- Custom TCP protocols secured by TLS

All the certificates for the different protocols can be managed in the Security Screen of Automation Builder, accessible via the icon 🗂 in the status bar or via the View menu.
FTP and FTPS

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

A 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:**

- 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:
- 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:
- 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
Encrypted Communication between engineering software and PLC

Together with Automation Builder the use of certificates for extended security can be activated and configured by the Security Screen (accessible via ☰️) in Automation Builder.

After enforcing of encrypted communication, the server certificate of the controller is used for establishing an encrypted connection. Then the entire communication is encrypted.

Recommendation:

- Use the secure online protocol for connecting to the PLC with Automation Builder
4.2 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.

Example 1: Connection of single controller

AC500 works as IoT-Gateway and is directly connected to the cloud. Security is established through TLS-encryption.

Benefits:
- No additional gateway required
- Low latency

Use Case:
Small systems with non-critical data transfer.
Example 2: 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.

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

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

Cisco provides a Device Access Checklist which can be found here.

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 upper and lower case 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 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
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AB</strong></td>
<td>Automation Builder</td>
</tr>
<tr>
<td><strong>Broken Authentication</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>CA</strong></td>
<td>Certification Authority</td>
</tr>
<tr>
<td><strong>Cross Site Scripting (XSS)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>FTP Bounce Attack</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>FTP Brute Force Attack</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>ICS</strong></td>
<td>Industrial Control Systems</td>
</tr>
<tr>
<td><strong>IT</strong></td>
<td>Information Technology</td>
</tr>
<tr>
<td><strong>LAN</strong></td>
<td>Local Area Network</td>
</tr>
<tr>
<td><strong>MCSR</strong></td>
<td>Minimum Cyber Security Requirements</td>
</tr>
<tr>
<td><strong>OT</strong></td>
<td>Operating Technology</td>
</tr>
<tr>
<td><strong>Packet Capture (Sniffing)</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>PGP</strong></td>
<td>Pretty Good Privacy. It's a public key block.</td>
</tr>
<tr>
<td><strong>Port Stealing</strong></td>
<td>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.</td>
</tr>
<tr>
<td>Security Misconfiguration</td>
<td>Security misconfiguration often using defaults that were not changed like keys and passwords</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Spoof Attack</td>
<td>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.</td>
</tr>
<tr>
<td>SQL injection</td>
<td>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. Read more</td>
</tr>
<tr>
<td>SSL</td>
<td>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.</td>
</tr>
<tr>
<td>TLS</td>
<td>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.</td>
</tr>
</tbody>
</table>
8 References

tID=6VZZ000367T00276&LanguageCode=en&DocumentPartId=&Action=Launch
3. https://mcuoneclipse.com/2017/04/14/enable-secure-communication-with-tls-and-
the-mosquitto-broker/
4. https://library.e.abb.com/public/d005b0262c3b4db8b6b2c2580eb0d3ad/Cyber%20robustness%20test-
ing%20flyer%20final.pdf
5. https://mcuoneclipse.com/2017/04/14/introduction-to-security-and-tls-transport-
security-layer/