APPLICATION NOTE

AC500 CYBER SECURITY

FAQS

Contents

1 Introduction

1.1 Scope of the document

The most raised questions, regarding AC500 Cyber Security are listed here. Please check our Whitepaper for further information. Some additional information can be found in the Automation Builder documentation:

- AC500 V2 Manual
- AC500 V3 Manual

1.2 Compatibility

The application notes and information's explained in this document have been used with the below engineering system versions. They should also work with other versions, nevertheless some small adaptations may be necessary, for future versions.

- AC500 V2 PLC **(V2.8.5)**
- AC500 V3 PLC **(V3.4.0.304)**
- Automation Builder **(V2.4.0.929)**

2 FAQs

Here is a list of most asked questions.

2.1 Cyber Security – General Requirements

2.1.1 How is Cybersecurity organized in AC500?

We take all necessary measures to continuously improve the security of the AC500.

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.

The AC500 provides certificates using TLS v1.2 standard to encrypt the connection from the PLC e.g. OPC UA Server to the OPC UA client.

We highly recommend that all software, firmware, libraries and applications are kept up to date using the most recent firmware and software updates to keep your system and environment secure.

2.2 Cyber Security – Device Security

2.2.1 What security measures are provided

Please find below a list of available features for AC500 V2 and AC500 V3 PLCs. We recommend using a AC500 V3 PLC. These PLC typed provide more security functionalities than the AC500 V2 PLC range.

- **AC500 V2 PLCs (PM5xx):**
  - Minimal amount of open ports by default
  - Secure communication protocols where possible:
    - MQTT with TLS
- **AC500 V3 PLCs (PM56xx):**
  - Digitally signed firmware updates
  - Minimal amount of open ports by default
  - Secure communication protocols where possible:
    - OPC UA communication with encryption
    - FTPS
    - HTTPS (for web visualization)
    - Secure communication between PLC and engineering system
    - MQTT with TLS
    - Customer protocols using TLS sockets

    Redirect is supported. You can forward for example an incoming connection from port 80(HTTP) to port 443(HTTPS)
  - Optional user rights management for different aspects of the system (project, PLC, Visualization)

2.2.2 User management in the Automation Builder and in the AC500

Please find a link to the Application Note: User management

2.2.3 Encrypt and Sign your Application

Please find a link to the Application Note: Encrypt and Sign your Application

2.2.4 What cyber security measurements are taken?

We test all devices in the ABB device security assurance center (DSAC) against various known vulnerabilities, do robustness testing and fuzzing of all protocols using well-known tools from different companies.
Please check our Whitepaper for further information.

2.2.5 What default ports are required in the PLC?

Ports can be configured freely for most protocols. This depends completely on the customer configuration and intensions.

The device only has a small set of default ports open for initial discovery and setup:

- UDP 24576 (device discovery and IP setup)
- TCP 11740 (communication ports for the engineering tool “Automation Builder”)

2.2.6 Do your devices report physical failures or temporary network interruptions?

Apart from the physical display and status LEDs, an out-of-band monitoring would have to be created via another fieldbus or similar communication ports, depending on the use case.

In addition, you can check the HA library:

- PS5601-HA-MTCP (will be installed with AB on local computer)

2.2.7 Do you support TLS?

Yes, we are supporting TLS 1.2 in our AC500 V2 and AC500 V3 PLCs.

2.2.8 Do you support 802.1x?

802.1x is currently not supported.

2.2.9 Do you support SSH access?

SSH is only used for support/developer access. Not enabled by default, protected by device-unique password.
For further information please check:

- AC500 V3 Manual

2.2.10 Do you support EAP-TLS?

EAP-TLS is currently not supported.

2.2.11 What encryption standards are available?

Current generation supports TLS 1.2 including cipher suites like ChaCha20 etc. With each firmware update we keep the cipher suites up to date.

2.2.12 Are asymmetric key algorithms supported?

Asymmetric Cryptography is available in AC500 V3 PLC but not for special protocol.

2.2.13 Are symmetric key algorithms supported?

Symmetric Cryptography is available in AC500 V3 PLC but not for special protocol.

2.2.14 Are cryptographic hash algorithms are supported?

Hash algorithms are available in AC500 V3. Please check the following libraries:

- CmpCrypto
- CmpX509Cert

2.2.15 Are Cryptographic algorithms require a cryptographically secure random number supported?

Randomness is available but not TRNG (True Random Number Generator).

2.2.16 Do you support MUD?

MUD (Manufacturer Usage Descriptions) is a new proposal by Cisco. Not supported.

2.2.17 Do you support automatic rollback to the previous firmware if the loaded firmware failed?

Before the update starts, the signature file will be checked. If there is a power loss during updating, this may cause a defect of the PLC. There is no rollback available.

2.2.18 Do you support event logs?

Event logs are limited supported.

2.2.19 Do you support physical intrusion protection system?

No, we do not support this. Be sure the PLC is located in a secure environment, where only trained persons should have access.
For further information please check:

- Whitepaper
- AC500 V2 Manual
- AC500 V3 Manual

2.2.20 Does the AC500 has his own PKI?

We are supporting PKI in this way, that we can import/export and create X509 certificates. The AC500 PLC can integrated and work together with an PKI.

2.2.21 Does the AC500 support OSCP?

The Online Certificate Status Protocol (OCSP) is a network protocol that enables clients to query the status of X.509 certificates from a validation service.
Certificates will be checked only offline not checked with an external server

2.3 Certification

2.3.1 Information's about Achilles

We are testing each firmware accordingly Achilles Level 1 and Level 2 – certificate will be most probably end of 2020 in place.
Please check our Whitepaper for further information.

2.3.2 Information's about IEC62443-4-1

We are pleased to announce that TÜV SÜD has certified the site ABB Automation Products GmbH (APR) in Heidelberg in accordance with the **IEC 62443-4-1:2018** standard. The certificate is a confirmation that APR develops Secure-by-design products in accordance with the IEC 62443-4-1 process.

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

2.3.3 Information's about IEC62443-4-2

We are working on IEC62443-4-2.

We are aiming to receive the certificate in Q2 2022.

2.3.4 Information's about CSPN

We are following IEC 62443-4-x.
This covers same scope on international level.

2.3.5 Information's about ISO 27001

We currently checking the requirements for ISO 270001.

2.4 Application

2.4.1 Can data be stored in an encrypted format?

Customers can use crypto libraries to en-/decrypt their own data. Please check the following libraries:

- CmpCrypto
- CmpX509Cert

2.4.2 Can we protect the human access to the device?

Access to data memory is only possible via engineering system or custom protocols, which can be secured using user rights management and secure connections via TLS.

2.4.3 Can we authenticate each device?

Yes, with OPC UA this can be archived. Also some brokers in the internet support bidirectional authorization.

2.4.4 Can we disable unused features and interfaces like FTP or webserver?

By default, all interfaces are disabled. The user customer need to manually activate the webserver or FTP server. Only Online Access is possible to login to the PLC.

We recommend using secure functionalities. This means use HTTPS instead of HTTP or FTPS instead of FTP.

2.4.5 Is a firewall implemented in the PLC?

We have no firewall implemented.

2.4.6 Do you support whitelisting and blacklisting?

No, we do not support both.

2.4.7 Do you support Secure Remote Access via VPN?

Please find a link to the Application Note: Secure remote access via Secomea gateway

2.4.8 Do you support Configuration versioning?

We are support SVN. This is an additional package, what can be installed via Automation Builder installation.

2.4.9 Do we have a security risk when we are using Mqtt?

When we are using Mqtt, the PLC act as client, this means, a connection will be established from the PLC to the broker. There is no open socket from outside, who someone else can connect. The PLC acting as client only in this case. No server functionality.

2.4.10 Can we encrypt the communication between the controller and the Engineering station?

Please use encrypted communication.

Please find a link to the Application Note: User management
Please find a link to the Application Note: Encrypt and Sign your Application

2.4.11 Can we checking for Integrity and correctness of the information transmitted? Like IPSEC protocol.

It’s recommended to use OPC UA together with TLS encryption.

2.4.12 Are you supporting SYSLOG in order of logging of any security exception e.g. unauthorized communication attempts?

This is ongoing. We planning to introduce this feature in Automation Builder V2.5, target end of 2021

2.4.13 Are you checking the integrity and uniformity of the controller's internal operating at each startup?

This is ongoing. We planning to introduce this feature in Automation Builder V2.5, target end of 2021. Secure boot is not available.

2.4.14 Can we check the integrity and uniformity of the application program?

Please use signed boot project.

Please find a link to the Application Note: Encrypt and Sign your Application

2.4.15 Can we block access to ethernet network services like: FTP / HTTP etc.?

Default and simple setting of controller and engineering is for all protocols off/disabled, only if protocols will be added, the communication port will be enabled.
See also What default ports are required in the PLC?

2.4.16 Can different users be identified and authenticated?

Yes, we can. For further details find a link to the Application Note: User management

2.4.17 Can we adapt the different user permissions?

Yes, we can. Please find a link to the Application Note: User management

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

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB AG does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents – in whole or in parts – is forbidden without prior written consent of ABB AG.
Copyright© 2021 ABB. All rights reserved