APPLICATION NOTE: **AN-0764**

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 web help

Be aware than the AC500 V3 provide much for security functionalities than the AC500 V2 PLC. Therefore, it is highly recommended to continue with AC500 V3 PLC.

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

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

The following

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 V3 PLC

Please find a link to the Application Note: User management

2.2.3 Encrypt and Sign your Application in the AC500 V3 PLC

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 AC500 V3 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:

- https://help.plc.abb.com/

2.2.10 Do you support EAP-TLS?

EAP-TLS is currently not supported.

2.2.11 Do you support EAP-Forwarding?

EAP-Forwarding is currently not supported.

2.2.12 Do you support EAP-Proxy-Logoff?

EAP-Proxy-Logoff is currently not supported.

2.2.13 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.

2.2.14 Are asymmetric key algorithms supported?

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

2.2.15 Are symmetric key algorithms supported?

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

2.2.16 Are cryptographic hash algorithms are supported?

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

- CmpCrypto
- CmpX509Cert

2.2.17 Are Cryptographic algorithms supported that require a cryptographically secure random number?

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

2.2.18 Do you support MUD?

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

2.2.19 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.

2.2.20 Do you support Audit Log?

Audit Logs are limited supported e.g. Login attempts, Download of application.

2.2.21 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 (web help)

2.2.22 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.

2.2.23 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 IEC62443-4-1

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 ABB Heidelberg 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.**
The 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

2.3.2 Information's about IEC62443-4-2

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

2.3.3 Information's about ISO 27001

Bureau Veritas has certificated site ABB AG in Heidelberg accordance with the ISO27001 standard.

The certificate can be found here:

Certificate

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.

Please find attached the whitepaper for differentiate between ISO 27000 and IEC62443:

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

2.3.4 Information's about Achilles

We are testing each firmware accordingly Achilles Level I and Level II
Please check our Whitepaper for further information.
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

2.3.5 Information's about CSPN

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

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 for AC500 V3 PLCs only:

- 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 needs 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 in AC500 V3 PLCs?

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 Audit Log in order of logging of any security exception e.g. unauthorized communication attempts?

Audit Log is supported with AB V2.5.0 and above.

2.4.13 Send Audit Log events to server?

Currently we cannot send Audit Log events to a dedicated server.

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

This is supported with AB V2.5.0 and above.

2.4.15 Do you support secure boot?

Secure boot is not available.

2.4.16 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

2.4.17 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?

2.4.18 Can different users be identified and authenticated in AC500 V3 PLCs?

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

2.4.19 Can we adapt the different user permissions?

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

2.4.20 Who is responsible when a customer is developing own libraries on top of your AC500 base offering?

You will have responsible for your self-created libraries. Therefore, they should follow the rules of IEC62443-4-2 (component) or IEC62443-3 (system).

We are also not certifying our libraries. We just certifying our product the AC500 V3 PLC.

If you sell your “application (libraries and PLC)” as own product/system, then you need to check with TÜV or any other certification agency if you need to certify your product again.

Either for product IEC62443-4-2 or as system for IEC62443-3-1/2/3.

2.4.21 Do we need to do any additional certification steps for the libraries or is it sufficient that the base platform for AC500 is certified?

This depends on your customer. On our IEC62443-4-2 certificate will be written that our AC500 V3 PLC with the dedicated firmware version is certified.

If you customer is satisfied with that, everything is fine.

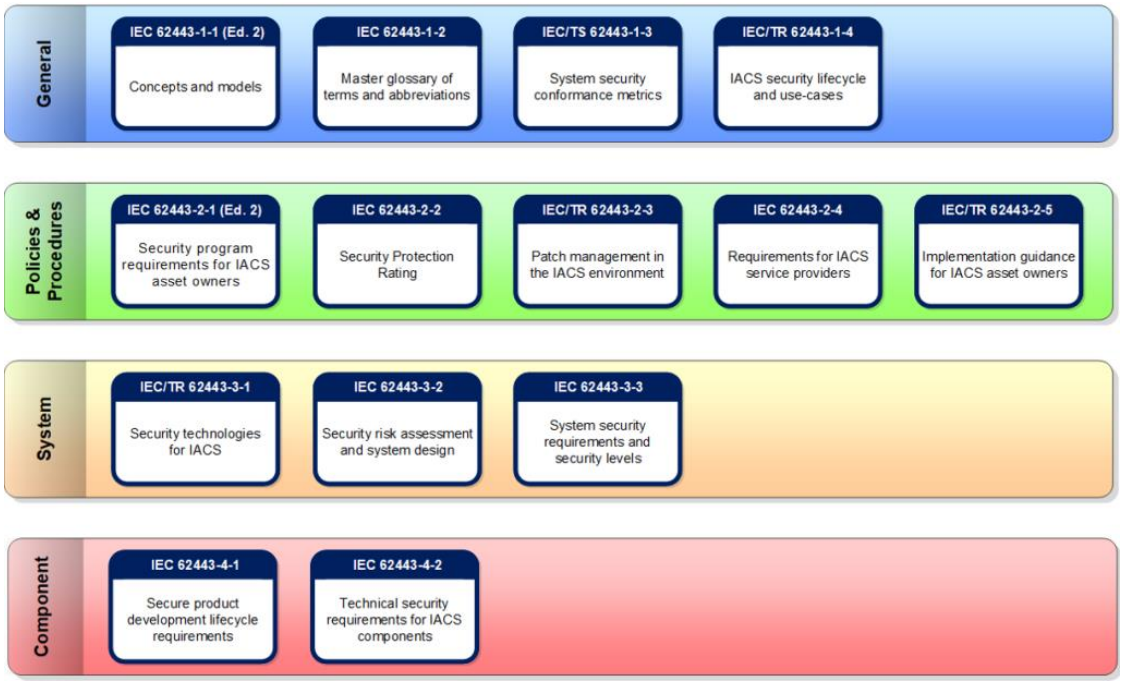
In case your customers want to see a certificate there AC500 EAU is IEC62443-4-2 is certified you need to do the additional steps.

As mentioned above the libraries itself will not be certified.

2.4.22 What would the additional 4-2 certification mean in terms of transfer prices? Would you add a library for 4-2 as an add-on layer?

Only the AC500 V3 product get certified. There will be no additional libraries, but we will check if we could provide some guidance for library development with principals to be considered.

In general, the IEC62443-3-1/2/3 will describe the need for system.



Link: https://www.hudsoncybertec.com/de/iec-62443/iec-62443-norm/

2.4.23 How is the software and firmware protected against malicious code?

ABB takes appropriate measures to protect any software deliverables from malware. This includes technical controls to scan the software with a minimum of 3 different up-to-date anti-malware solutions before delivery.

2.5 Unsecure Protocols

2.5.1 During the commissioning of my automation system tenable Nessus vulnerability scanner discovered three Modbus TCP vulnerabilities. Do we have a security risk when we are using Modbus TCP?

AC500 does not support a secure/encrypted variant of the Modbus TCP protocol. The hardening of systems using non-secure protocols must be done with additional measures like a proper defense in depth, network segmentation and additional firewall. For further information see Whitepaper.

2.5.2 During the commissioning of my automation system tenable Nessus vulnerability scanner discovered the vulnerability 10114 - ICMP Timestamp Request Remote Date Disclosure. Does the AC500 PLC has a security risk?

The remote host answers to an ICMP timestamp request. This allows an attacker to know the date that is set on the targeted machine, which may assist an unauthenticated, remote attacker in defeating time-based authentication protocols. AC500 doesn't support time-based authentication protocols.

ABB AG

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

Homepage:
www.abb.com/plc