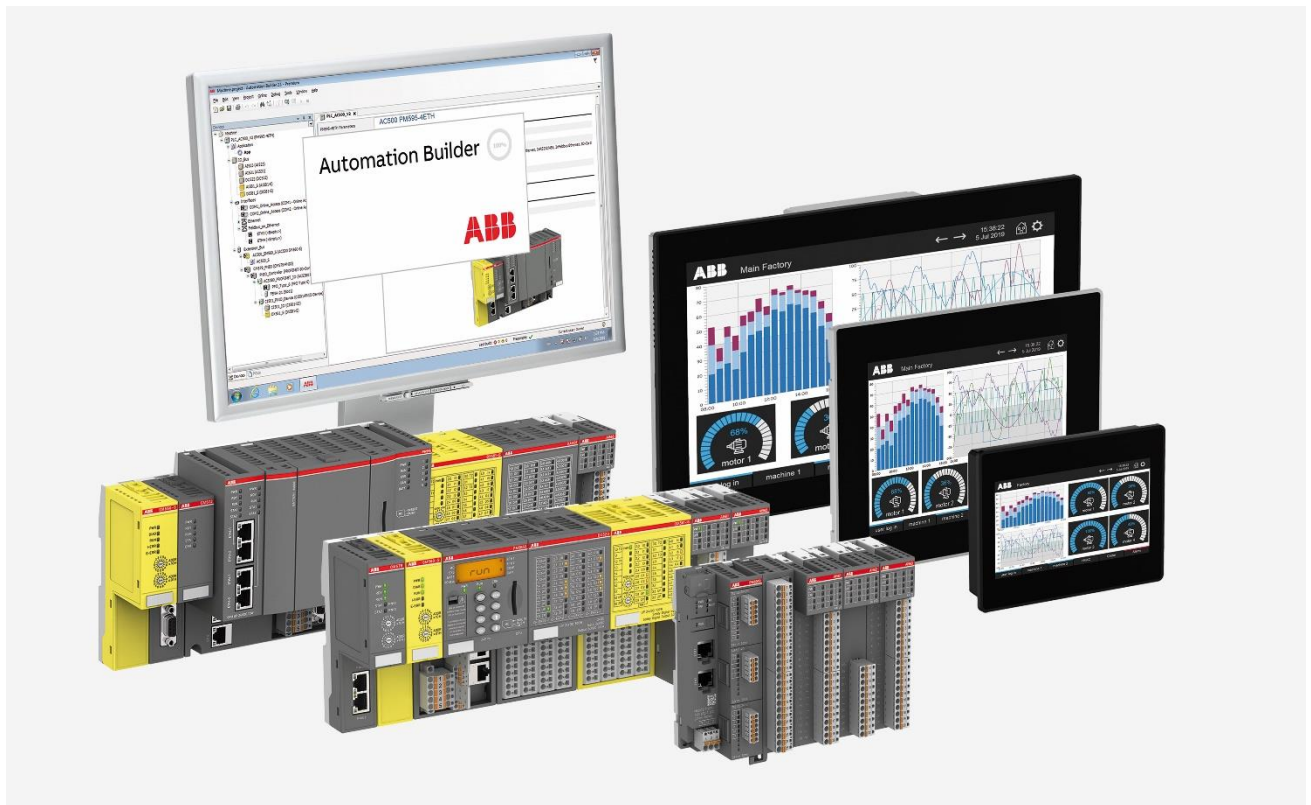


APPLICATION NOTE: AN-1330

AC500 CYBER SECURITY

SECURITY LEVEL CAPABILITIES ACCORDING TO IEC 62443-4-2



Contents

1 Introduction	3
1.1 Scope of the document	3
2 Overview of AC500 Security Level Capabilities	4
2.1 Overview of AC500 Security Level Capability.....	4

1 Introduction

1.1 Scope of the document

AC500 V3 PLC is certified according to parts of the [IEC 62443 standard](#), defining requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS). In particular, AC500 V3 PLC has the following certifications:

- [IEC 62443-4-1 - Certification of secure lifecycle development](#)
 - The AC500 V3 development process is compliant to the IEC443-4-1 with ML (maturity level) of either 3 or 4, depending on the requirement
- [IEC 62443-4-2 - Certification of industrial control systems and components](#)
 - The AC500 V3 PLC is compliant with the IEC 62443-4-2 SL-C (Security Level Capability) 1
 - The AC500 V3 PLC is fully aligned with the IEC 62443-4-2 SL-C 2
 - There are deviations in the AC500 V3 specific implementation of the requirement „Authenticity of the boot process “(EDR 3.14 RE1) compared to the standard.
 - AC500 V3 PLC is compliant with SL-C 2 regarding all other requirements
- Further information about secure use of our products is available from the cyber security chapter of the manual and from our [White Paper - AC500 Cyber Security](#).
- The most raised questions, regarding AC500 Cyber Security are listed in our [AC500 Cyber Security - FAQs](#)


2 Overview of AC500 Security Level Capabilities

The AC500 V3 and AC500-eCo V3 PLC Series are IEC62443-4-2 certified from FW Version 3.6.2 with the security level capability shown in the table below.

Legend:

●	Fulfilled Requirements
○	Fulfilled Requirements with Limitations (May require additional measures on system level)
—	Not Fulfilled Requirements
N/A	Not applicable Requirements

Note

	Note: Some requirements are already fulfilled by newer firmware version but not yet certified by the TÜV SÜD. See column Remark for the related items.
--	--

2.1 Overview of AC500 Security Level Capability

Item	Description	SL-C 1	SL-C 2	SL-C 3	SL-C 4	Fulfillment	Remark
FR 1	Identification and authentication control						
CR1.1	Human user identification and authentication	x	x	x	x	●	
CR1.1 RE(1)	Unique identification and authentication		x	x	x	○	Limitation for FTP server
CR1.1 RE(2)	Multifactor authentication for all interfaces			x	x	—	
CR1.2	Software process and device identification and authentication		x	x	x	●	
CR 1.2 RE(1)	Unique identification and authentication			x	x	—	

CR 1.3	Account management	x	x	x	x		
CR 1.4	Identifier management	x	x	x	x		
CR 1.5	Authenticator management	x	x	x	x		
CR 1.5 RE(1)	Hardware security for authenticators			x	x		
CR 1.6	Wireless access management					N/A	component specific, N/A for EDR
CR 1.7	Strength of password-based authentication	x	x	x	x		Available from FW3.7.x
CR 1.7 RE(1)	Password generation and lifetime restrictions for human users			x	x		
CR 1.7 RE(2)	Password lifetime restrictions for all users (human, software process, or device)				x		
CR 1.8	Public key infrastructure certificates		x	x	x		
CR 1.9	Strength of public key-based authentication		x	x	x		
CR 1.9 RE(1)	Hardware security for public key-based authentication			x	x		
CR 1.10	Authenticator feedback	x	x	x	x		Available from FW3.7.x
CR 1.11	Unsuccessful login attempts	x	x	x	x		Available from FW3.7.x
CR 1.12	System use notification	x	x	x	x		
CR 1.13	Access via untrusted networks					N/A	component-specific, N/A for EDR
CR 1.14	Strength of symmetric key-based authentication		x	x	x	N/A	
CR 1.14 RE(1)	Hardware security for symmetric key-based authentication			x	x	N/A	
FR 2	Use control						

CR 2.1	Authorization enforcement	x	x	x	x	●	
CR 2.1 RE(1)	Authorization enforcement for all users (humans, software processes and devices)		x	x	x	●	
CR 2.1 RE(2)	Permission mapping to roles		x	x	x	●	
CR 2.1 RE(3)	Supervisor override			x	x	—	
CR 2.1 RE(4)	Dual approval				x	—	
CR 2.2	Wireless use control	x	x	x	x	N/A	No wireless interface
CR 2.3	Use control for portable and mobile devices					N/A	No component level requirement associated with IEC 62443-3-3 SR 2.3
CR 2.4	Mobile code					N/A	See EDR 2.4
CR 2.5	Session lock	x	x	x	x	●	
CR 2.6	Remote session termination		x	x	x	●	
CR 2.7	Concurrent session control			x	x	—	
CR 2.8	Auditable events	x	x	x	x	●	
CR 2.9	Audit storage capacity	x	x	x	x	●	
CR 2.9 RE(1)	Warn when audit record storage capacity threshold reached			x	x	—	
CR 2.10	Response to audit processing failures	x	x	x	x	●	
CR 2.11	Timestamps	x	x	x	x	●	
CR 2.11 RE(1)	Time synchronization		x	x	x	●	

CR 2.11 RE(2)	Protection of time source integrity				x	—	
CR 2.12	Non-repudiation	x	x	x	x	●	
CR 2.12 RE(1)	Non-repudiation for all users				x	—	
CR 2.13	Use of physical diagnostic and test interfaces					●	See EDR 2.13
FR 3	System integrity						
CR 3.1	Communication integrity	x	x	x	x	●	
CR 3.1 RE(1)	Communication authentication		x	x	x	●	
CR 3.2	Protection from malicious code	x	x	x	x	○	Available from FW3.7.x
CR 3.3	Security functionality verification	x	x	x	x	●	
CR 3.3 RE(1)	Security functionality verification during normal operation				x	—	
CR 3.4	Software and information integrity	x	x	x	x	●	
CR 3.4 RE(1)	Authenticity of software and information		x	x	x	●	
CR 3.4 RE(2)	Automated notification of integrity violations			x	x	—	
CR 3.5	Input validation	x	x	x	x	○	
CR 3.6	Deterministic output	x	x	x	x	●	
CR 3.7	Error handling	x	x	x	x	●	
CR 3.8	Session integrity		x	x	x	●	
CR 3.9	Protection of audit information		x	x	x	●	
CR 3.9 RE(1)	Audit records on write-once media				x	—	

CR 3.10	Support for updates						●	See EDR 3.10
CR 3.11	Physical tamper resistance and detection						●	See EDR 3.11
CR 3.12	Provisioning product supplier roots of trust						●	See EDR 3.12
CR 3.13	Provisioning asset owner roots of trust						●	See EDR 3.13
CR 3.14	Integrity of the boot process						●	See EDR 3.14
FR 4	Data confidentiality							
CR 4.1	Information confidentiality	x	x	x	x		●	
CR 4.2	Information persistence		x	x	x		●	
CR 4.2 RE(1)	Erase of shared memory resources			x	x		—	
CR 4.2 RE(2)	Erase verification			x	x		—	
CR 4.3	Use of cryptography	x	x	x	x		●	
FR 5	Restricted data flow							
CR 5.1	Network segmentation	x	x	x	x		●	
CR 5.2	Zone boundary protection						N/A	Network-component-specific
CR 5.3	General-purpose person-to-person communication restrictions						N/A	Network-component-specific
CR 5.4	Application partitioning						N/A	No component level requirement associated with IEC 62443-3-3 SR 5.4
FR 6	Timely response to events							
CR 6.1	Audit log accessibility	x	x	x	x		●	

CR 6.1 RE(1)	Programmatic access to audit logs			x	x	—	
CR 6.2	Continuous monitoring		x	x	x	●	
FR 7	Resource availability						
CR 7.1	Denial of service protection	x	x	x	x	●	
CR 7.1 RE(1)	Manage communication load from component		x	x	x	●	
CR 7.2	Resource management	x	x	x	x	●	
CR 7.3	Control system backup	x	x	x	x	●	
CR 7.3 RE(1)	Backup integrity verification		x	x	x	●	
CR 7.4	Control system recovery and reconstitution	x	x	x	x	●	
CR 7.5	Emergency power					N/A	No component level requirement associated with IEC 62443-3-3 SR 7.5
CR 7.6	Network and security configuration settings	x	x	x	x	●	
CR 7.6 RE(1)	Machine-readable reporting of current security settings			x	x	—	
CCR 7.7	Least functionality	x	x	x	x	●	
CR 7.8	Control system component inventory		x	x	x	●	
EDR 2	Embedded device requirements						
EDR 2.4	Mobile code	x	x	x	x	N/A	No mobile code used
EDR 2.4 RE(1)	Mobile code authenticity check		x	x	x	N/A	No mobile code used
EDR 2.13	Use of physical diagnostic and test interfaces		x	x	x	●	

EDR 2.13 RE(1)	Active monitoring			x	x	—	
EDR3.2	Protection from malicious code	x	x	x	x	●	Available from FW3.7.x
EDR 3.10	Support for updates	x	x	x	x	●	
EDR 3.10 RE(1)	Update authenticity and integrity		x	x	x	●	
EDR 3.11	Physical tamper resistance and detection		x	x	x	●	Basic tamper resistance, Device must be installed in access restricted environment (e.g. locked cabinet)
EDR 3.11 RE(1)	Notification of a tampering attempt			x	x	—	
EDR 3.12	Provisioning product supplier roots of trust		x	x	x	●	
EDR 3.13	Provisioning asset owner roots of trust		x	x	x	●	
EDR 3.14	Integrity of the boot process	x	x	x	x	●	
EDR 3.14 RE(1)	Authenticity of the boot process		x	x	x	—	

ABB AG

Contact:

<https://access.motion.abb.com/contact/contact>

Homepage:

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© 2024 ABB. All rights reserved.