

Req ID	Requirement name	Supported by CIP	Need applicability	Status if supported	HW solution	IEC-62443-4-2 tests reference	CIP recommendation
CR-3.1	Communication integrity	TRUE	TRUE	FALSE	Completed	Refer to CR-3.1	<b>Default Action</b> The platform provides capabilities for secure communication, application needs to use them
CR-3.1	Communication authentication	TRUE	TRUE	FALSE	Completed	Refer to CR-3.1	Same as CR-3.1
SAR-3.2	Protection from malicious code	FALSE	FALSE	FALSE	N/A.	None	This requirement is only for Software application
EDR-3.2	Protection from malicious code	FALSE	TRUE	FALSE	N/A.	None	CIP does not support this requirement. SYSTEM: Use a combination of detection and prevention techniques to protect the system from installation and execution of unauthorized software. We recommend all software to be signed by its trusted source and to use whitelisting and ACL to prevent execution of unknown software. Secure boot can also be useful to ensure system integrity. Disabling portable storage device auto-mount function in default is recommended.
HDR-3.2	Protection from malicious code	FALSE	FALSE	FALSE	N/A.	None	SYSTEM: Use a combination of detection and prevention techniques to protect the system from installation and execution of unauthorized software. We recommend all software to be signed by its trusted source and to use whitelisting and ACL to prevent execution of unknown software. Secure boot can also be useful to ensure system integrity. Disabling portable storage device auto-mount function in default is recommended.
HDR-3.2	Report version of code protection	FALSE	FALSE	FALSE	N/A.	None	APP: Need to automatically report the version of signatures of software for protection from malicious code. However, this requirement assumes the installation of anti-virus software provided for general-purpose operating systems such as Windows. If you install a specific anti-virus software, you need to log also its version.

Req ID	Requirement name	Supported by CIP	Need application HW solution	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation	
NDR-3.2	Protection from malicious code	FALSE	TRUE	FALSE	SL-4	None	CIP does not support this requirement. SYSTEM: Network devices need to either be protected from malicious code by external compensation control or need internal protection from malicious code like in HDR 3.2/EDR 3.2. However, even if the network device itself takes measures, it is recommended to keep it lightweight so that the throughput is not affected.
CR-3.3	Security functionality verification	FALSE	TRUE	FALSE	SL-4	None	CIP does not support this requirement. CIP users should verify the security functionality supported by the product according to this requirement
CR-3.3 RE(1)	Security functionality verification during normal operation	FALSE	FALSE	FALSE	SL-4	None	This is for SL-4
CR-3.4	Software and information integrity	TRUE	TRUE	FALSE	Completed packages openssl, aide, aide-common	<a href="https://gitlab.com/ieda/ieda-project/cip-testing/cip-security-aide-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR3.4_1">https://gitlab.com/ieda/ieda-project/cip-testing/cip-security-aide-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR3.4_1</a>	CIP supports this requirement. However, application developer need to verify the integrity of software and configuration
CR-3.4 RE(1)	Authenticity of software and information	TRUE	TRUE	FALSE	Same as CR-3.4	<a href="https://gitlab.com/ieda/ieda-project/cip-testing/cip-security-aide-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR3.4-RE1_1">https://gitlab.com/ieda/ieda-project/cip-testing/cip-security-aide-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR3.4-RE1_1</a>	Same as CR-3.4

Req ID	Requirement name	Supported by CIP	Need supported by HW	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation	
CR-3.4 RE(2)	Automated notification of integrity violations	TRUE	TRUE	FALSE	Completed by syslog package	Added digital signature as CR-3.4 Any mismatch in integrity data such as hash or checksum should be notified to other layers as well as logged for audit purpose. Once checksum or digital verification is failed, depending upon which layer it failed, the system needs to determine how to handle it, <a href="#">https://github.com/industrialproject/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR3.4-RE2_1</a>	
CR-3.5	Input validation	TRUE	TRUE	FALSE	N.A.	None	CIP users to make sure all the interfaces do input validation such as input for industrial process control, input via external interfaces
CR-3.6	Determine output	FALSE	TRUE	FALSE	N.A.	None	CIP does not support this requirement. CIP user should make sure it is met by application. Meeting this requirement is full responsibility of CIP user
CR-3.7	Error handling	TRUE	TRUE	FALSE	Added syslog	None	CIP ensures no confidential information is exposed in logs which can be exploited by adversaries. CIP users should ensure any sensitive information is not printed in the logs.
CR-3.8	Session integrity	TRUE	TRUE	FALSE	Completed by openssl package	Added openssl tests in CR1.9	CIP platform provides low level package for session integrity. Application developers should use platform capabilities to protect application sessions.
CR-3.9	Protection of audit information	TRUE	FALSE	FALSE	Completed by package acl	Added digital signature <a href="#">https://github.com/industrialproject/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR3.9_1</a>	<a href="#">In CIP Action</a>
CR-3.9 RE(1)	Audit records write-once media	FALSE	FALSE	FALSE	N.A.	None	For SL-4
EDR-3.10	Support for updates	TRUE	TRUE	FALSE	In progress	None	CIP provides reference implementation for software updates. However, CIP does not provide any software update for CIP users or devices. CIP users can use CIP software update as reference implementation and develop software updates based on their requirements.

Req ID	Requirement name	Supported by CIP	Need application HW solution	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
EDR-3.10	Update authenticity and integrity	TRUE	FALSE	In-progress	None	Same as EDR-3.10
HDR-3.10	Support for updates	FALSE	TRUE	N.A.	None	This is for host devices not supported by CIP
HDR-3.10	Update authenticity and integrity	FALSE	TRUE	N.A.	None	This is for host devices not supported by CIP
NDR-3.10	Support for updates	TRUE	FALSE	In-progress	None	Same as EDR-3.10
NDR-3.10	Update authenticity and integrity	TRUE	FALSE	In-progress	None	Same as EDR-3.10
EDR-3.11	Physical tamper resistance and detection	FALSE	FALSE	TRUE	N.A.	Requires HW support
EDR-3.11	Notification of a tampering attempt	FALSE	TRUE	N.A.	None	CIP does not support this requirement. CIP users should support this requirement.
HDR-3.11	Physical tamper resistance and detection	FALSE	FALSE	TRUE	N.A.	This is for host devices

Req ID	Requirement name	Supported by CIP	Need application HW solution	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
HDR-3.11 RE(1)	Notification tampering attempt	FALSE	TRUE	N.A.	None	This is for host devices
NDR-3.11	Physical tamper resistance and detection	FALSE	TRUE	N.A.	None	Requires HW support
NDR-3.11 RE(1)	Notification tampering attempt	FALSE	TRUE	N.A.	None	CIP does not support this requirement This requirement should be supported by CIP users
EDR-3.12	Provisioning product supplier roots of trust - protection	FALSE	TRUE	N.A.	None	CIP does not support this requirement.This will be supported by CIP users
HDR-3.12	Provisioning product supplier roots of trust - protection	FALSE	TRUE	N.A.	None	It's for host devices
NDR-3.12	Provisioning product supplier roots of trust - protection	FALSE	TRUE	N.A.	None	Same as EDR-3.12

Req ID	Requirement name	Supported by CIP	Need applicability	Status if supported	IEC-62443-4-2 tests reference	CIP recommendation
EDR-3.13	Provisioning of asset owner roots of trust - protection	FALSE	TRUE	None	None	CIP platform does not support this requirement. CIP users should support this requirement by using CIP capability.
HDR-3.13	Provisioning of asset owner roots of trust - protection	FALSE	TRUE	None	None	This is only applicable to host devices
NDR-3.13	Provisioning of asset owner roots of trust - protection	FALSE	TRUE	None	None	Same as EDR-3.13
EDR-3.14	Integrity of the boot process	FALSE	TRUE	In-progress	None	CIP provides reference implementation of secure boot. CIP users should meet it based on their secure hardware support.
EDR-3.14 RE(1)	Authenticity of the boot process	FALSE	TRUE	In-progress	None	CIP provides reference implementation of secure boot implementation. CIP users should meet it based on their secure hardware support.
HDR-3.14	Integrity of the boot process	FALSE	TRUE	None	None	It's for host devices
HDR-3.14 RE(1)	Authenticity of the boot process	FALSE	TRUE	None	None	It's for host devices
NDR-3.14	Integrity of the boot process	FALSE	TRUE	In-progress	None	CIP provides reference implementation of secure boot implementation. CIP users should meet it based on their secure hardware support.
NDR-3.14 RE(1)	Authenticity of the boot process	FALSE	TRUE	In-progress	None	CIP provides reference implementation of secure boot implementation. CIP users should meet it based on their secure hardware support.