Req ID	Requirement name	Supported by CIP	Need application support	Need HW support	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
CR-3.1	Communication integrity	TRUE	TRUE	FALSE	Completed	Refer added openssl CR1.9 package tests for openssl	Default ActionThe platform provides capabilities for secure communication, application needs to use them
CR 3.1 RE(1)	Communication authentication	TRUE	TRUE	FALSE	Completed	Refer added openssl CR1.9 package tests for openssl	Same as CR-3.1
SAR-3.2	Protection from malicious code	FALSE	FALSE	FALSE	SEA.	None	This requirement is only for Software application
EDR-3.2	Protection from malicious code	FALSE	TRUE	FALSE	SEA.	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.

Req ID	Requirement name	Support by CIP	Need application support	Need HW support	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
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 RE(1)	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.
NDR 3.2	Protection from malicious code	FALSE	TRUE	FALSE	N.A.	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.

Req ID	Requirement name	Supported by CIP	Need application support	Need HW support	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
CR-3.3	Security functionality verification	FALSE	TRUE	FALSE	SEA.	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	SEA.	None	This is for SL-4
CR-3.4	Software and information integrity	TRUE	TRUE	FALSE	Completed packages openssl, aide, aide-common	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR3.4_1	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	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR3.4-RE1_1	Same as CR-3.4

Req ID	Requirement name	Supported by CIP	Need application support	Need HW support	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	Supported via syslog-ng package	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/security-tests/singlenode-testcases/TC_CR3.4-RE2_1	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,
CR-3.5	Input validation	TRUE	TRUE	FALSE	SEA.	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	Determinism output	FALSE	TRUE	FALSE	SEA.	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-ng	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	Supported package openssl	Refer added 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	Supported package acl	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR3.9_1	Default action

Req ID	Requirement name	Supported by CIP	Need application support	Need HW support	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
CR-3.9 RE(1)	Audit records on 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.
EDR-3.10 RE(1)	Update authenticity and integrity	TRUE	TRUE	FALSE	In progress	None	Same as EDR-3.10
HDR-3.10	Support for updates	FALSE	TRUE	FALSE	N.A.	None	This is for host devices not supported by CIP
HDR-3.10 RE(1)	Update authenticity and integrity	FALSE	TRUE	FALSE	N.A.	None	This is for host devices not supported by CIP
NDR-3.10	Support for updates	TRUE	TRUE	FALSE	In progress	None	Same as EDR-3.10

Req ID	Requirement name	Supported by CIP	Need application support	Need HW solution	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
NDR 3.10 RE(1)	Update authenticity and integrity	TRUE	TRUE	FALSE	SE in progress	None	Same as EDR-3.10
EDR 3.11	Physical tamper resistance and detection	FALSE	FALSE	TRUE	N.A.	None	Requires HW support
EDR 3.11 RE(1)	Notification of a tampering attempt	FALSE	TRUE	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.	None	This is for host devices
HDR 3.11 RE(1)	Notification of a tampering attempt	FALSE	FALSE	TRUE	N.A.	None	This is for host devices

Req ID	Requirement name	Supported by CIP	Need application support	Need HW solution	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
NDR 3.11	Physical tamper resistance and detection	FALSE	FALSE	TRUE	N.A.	None	Requires HW support
NDR 3.11 RE(1)	Notification of a tampering attempt	FALSE	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	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	FALSE	TRUE	N.A.	None	It's for host devices

Req ID	Requirement name	Supported by CIP	Need application support	Status if supported	Need HW by CIP	IEC-62443-4-2 tests reference	CIP recommendation
NDR-3.12	Provisioning product supplier roots of trust - protection	FALSE	FALSE	TRUE	N.A.	None	Same as EDR-3.12
EDR-3.13	Provisioning asset owner roots of trust - protection	FALSE	TRUE	TRUE	N.A.	None	CIP platform does not support this requirement.CIP users should support this requirement by using CIP capability.
HDR-3.13	Provisioning asset owner roots of trust - protection	FALSE	FALSE	TRUE	N.A.	None	This is only applicable to host devices
NDR-3.13	Provisioning asset owner roots of trust - protection	FALSE	TRUE	TRUE	N.A.	None	Same as EDR-3.13

Req ID	Requirement name	Supported by CIP	Need application support	Need HW solution	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
EDR 3.14	Integrity of the boot process	FALSE	TRUE	TRUE	in-progress	None	CIP provides reference implementation of secure boot.CIP users should meet it it based on their secure hardware support.
EDR 3.14 RE(1)	Authenticity of the boot process	FALSE	TRUE	TRUE	in-progress	None	CIP provides reference implementation of secure boot implementation.CIP users should meet it it based on their secure hardware support.
HDR 3.14	Integrity of the boot process	FALSE	FALSE	TRUE	N.A.	None	It's for host devices
HDR 3.14 RE(1)	Authenticity of the boot process	FALSE	FALSE	TRUE	N.A.	None	It's for host devices
NDR 3.14	Integrity of the boot process	FALSE	FALSE	TRUE	in-progress	None	CIP provides reference implementation of secure boot implementation.CIP users should meet it it based on their secure hardware support.
NDR 3.14 RE(1)	Authenticity of the boot process	FALSE	FALSE	TRUE	in-progress	None	CIP provides reference implementation of secure boot implementation.CIP users should meet it it based on their secure hardware support.