Req ID	Requirement name	Supported by CIP	Need application HW support	Need application SW support	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
CR-1.1	Human user identification and authentication	TRUE	FALSE	FALSE	Completed and tested	Added https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.1_12. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.1_2	The CIP platform complies with this requirement. Users can login through various interfaces (e.g. serial console, http etc).CIP based products may use variety of interfaces, this requirement mandates on each interface user or process or device should be uniquely identified and authenticated.
CR-1.1 RE(1)	Unique identification and authentication	TRUE	FALSE	FALSE	Completed and tested	Added https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.1-RE1_1	Same as CR-1.1
CR-1.1 RE(2)	Multi-factor authentication for all interfaces	TRUE	FALSE	FALSE	Completed and tested	Adding libpam-google-authenticator	The CIP platform complies with this requirement by adding google MFA Debian package. However, CIP users can use their own way to achieve this MFA.

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-1.2	Software process and device identification and authentication	FALSE	TRUE	FALSE	SEA.	None	The CIP platform can't meet this requirement, CIP users should use their applications to meet this requirementAll components need to identify themselves. We recommend the usage of TPM generated id or certificates for device id, a process pid and the addition of the active user account. The pid must be logged in the processes lifetime as it changes after a process restart.
CR1.2-RE(1)	Unique identification and authentication	FALSE	TRUE	FALSE	SEA.	None	APP: All certificates/authentication ids for 1.2 need to be unique.
CR-1.3	Account management	TRUE	FALSE	SEA.	Completed	1. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.3_1 2. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.3_2 3. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.3_3	Default Action
CR-1.4	Identifier management	TRUE	FALSE	SEA.	Completed	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.4_1	Default Action

Req ID	Requirement name	Supported by CIP	Need application HW support	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
CR-1.5	Authenticator management - initialize authenticator content	TRUE	FALSE	SE	Completed	Added https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.5_22. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.5_3	Default Action
CR-1.5-RE(1)	The authenticators on which the company rely shall be protected via hardware mechanism	TRUE	FALSE	SE	Completed	None needed	This requirement expects a secure storage, CIP added TPM tools. However, secure storage and any other tools needed should be met by CIP users based on their requirements.
NDR 1.6	Wireless access management	TRUE	TRUE	FALSE	In-progress	None Wireless drivers to be included in CIP kernel	Default Action

Req ID	Requirement name	Supported by CIP	Need application HW support	Need application SW support	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
NDR 1.6 RE(1)	Unique identification and authentication	TRUE	TRUE	FALSE	In-progress	None	Default Action
CR-1.7	Strength of password-based authentication	TRUE	FALSE	SEA.	Completed	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.7_1	Default Action
CR-1.7 RE(1)	Password generation and lifetime restrictions for human users	TRUE	FALSE	SEA.	Completed	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.7-RE1_1	Default Action
CR-1.7 RE(2)	Password lifetime restrictions for all users (human, software process, or device)	FALSE	SEA.	SEA.	SEA.	None	This is for SL-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-1.8	Public key infrastructure (PKI) certificates	TRUE	FALSE	FALSE	Completed	Added https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.8_1	Default Action
CR-1.9	Strength of public key-based authentication - check validity of signature of a given certificate	TRUE	FALSE	FALSE	Completed	Added https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_12. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_23. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_34. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_45. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_56. https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.9_6	Default Action
CR-1.9 RE(1)	Hardware security for public key-based authentication	TRUE	FALSE	TRUE	Completed	Not tested	It requires HW support, should be met by CIP users
CR-1.10	Authenticator feedback	TRUE	FALSE	FALSE	Completed	Added https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR2.10_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-1.11	Unsuccessful login attempts - limit number	TRUE	FALSE	SE	Completed, added package libpam-modules-bin	https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.11_1 https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-security-tests/singlenode-testcases/TC_CR1.11_2	Default Action
CR-1.12	System use notification	FALSE	TRUE	FALSE	SEA.	None	CIP does not support this requirement, CIP users should implement notifications based on their requirements.Following are some guidelinesAPP: If the device has a HMI for an application requiring authentication, the application shall be able to display a configurable use notification message before the credentials are requested from the user.
NDA-1.13	Access via untrusted networks	FALSE	TRUE	FALSE	SEA.	None	CIP does not support this requirement.Access of networks should be monitored using network security software and tools, only used ports should be open and unused ports should be blocked to avoid unauthorized access.

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
NDR 1.13 RE(1)	Explicit access request approval	FALSE	TRUE	FALSE	N.A.	None	CIP does not support this requirement.Application based security policies, explicit request should be raised to access blocked URLs or ports to monitor them closely. Requests need to be approved by an assigned role. This can be done by a human or machine user.
CR-1.14	Strength of symmetric key-based authentication	TRUE	FALSE	FALSE	Completed/Added openssl package	https://github.com/cip-project/cip-testing/cip-security-tests/-/tree/master/iec-62443-security-tests/singlenode-testcases/TC_CR1.8_1	Default Action
CR-1.14 RE(1)	Hardware security for symmetric key-based authentication	TRUE	FALSE	TRUE	N.A.	None	Requires HW support