Req ID	Requirement name	Supported by CIP	Need application support	Need HW solution	Status if supported by CIP
CR-2.1	Authorization enforcement	TRUE	TRUE	FALSE	CompletedAdded acl package
CR-2.1 RE(1)	Authorization enforcement for all users (humans, software processes and devices)	TRUE	TRUE	FALSE	CompletedAdded acl package
CR-2.1 RE(2)	Permission mapping to roles	TRUE	TRUE	FALSE	CompletedAdded acl package
CR-2.1 RE(3)	Supervisor override	TRUE	TRUE	FALSE	CompletedAdded sudo package
CR-2.1 RE(4)	Dual approval	FALSE	FALSE	FALSE	N.A.
CR-2.2	Wireless use control	FALSE	TRUE	FALSE	N.A.
CR-2.3	Use control for portable and mobile devices	FALSE	FALSE	FALSE	N.A.
SAR-2.4	Mobile code	FALSE	FALSE	FALSE	N.A.
SAR-2.4 RE(1)	Mobile code - authenticity check	FALSE	TRUE	FALSE	N.A.
EDR-2.4	Mobile code	FALSE	TRUE	FALSE	N.A.
EDR-2.4 RE(1)	Mobile code - authenticity check	FALSE	TRUE	FALSE	N.A.
HDR-2.4	Mobile code	FALSE	TRUE	FALSE	N.A.
HDR-2.4 RE(1)	Mobile code - authenticity check	FALSE	TRUE	FALSE	N.A.
NDR-2.4	Mobile code	FALSE	TRUE	FALSE	N.A.
NDR-2.4 RE(1)	Mobile code - authenticity check	FALSE	TRUE	FALSE	N.A.
CR-2.5	Session lock	TRUE	TRUE	FALSE	CompletedAdded package openssh
CR-2.6	Remote session termination	TRUE	TRUE	FALSE	CompletedAdded package openssh
CR-2.7	Concurrent session control	TRUE	TRUE	FALSE	Completed Added pam and openssh package
CR-2.8	Auditable events	TRUE	TRUE	FALSE	CompletedAdded package auditd

Req ID	Requirement name	Supported by CIP	Need application support	Need HW solution	Status if supported by CIP
CR-2.9 RE(1)	Warn when audit record storage capacity threshold reached	TRUE	TRUE	FALSE	CompletedAdded package auditd and rsyslog
CR-2.10	Response to audit processing failures	TRUE	TRUE	FALSE	In-progress
CR-2.11	Timestamp	TRUE	FALSE	FALSE	CompletedAdded package chrony
CR-2.11 RE(1)	Time synchronization	TRUE	FALSE	FALSE	CompletedAdded package chrony
CR-2.11 RE(2)	Protection of time source integrity	FALSE	FALSE	FALSE	N.A.
CR-2.12	Non-repudiation	TRUE	TRUE	FALSE	CompletedAdded packages audits and syslog-ng
CR-2.12 RE(1)	Non-repudiation for all users	FALSE	FALSE	FALSE	N.A.
EDR-2.13	Use of physical diagnostic and test interfaces	FALSE	FALSE	TRUE	N.A.
EDR-2.13 RE(1)	Active monitoring	TRUE	TRUE	TRUE	CompletedAdded packages syslog-ng, auditd
HDR-2.13	Use of physical diagnostic and test interfaces	FALSE	FALSE	TRUE	N.A.
HDR-2.13 RE(1)	Active monitoring	TRUE	FALSE	TRUE	N.A.

Tests reference and CIP recommendation

Req ID	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
CR-2.1	CompletedAdded acl package	TC_CR2.1_1	Default ActionFor local interface, file and directory access control must be configured using ACL, chmod or a similar effective mechanism.For network interface, user should create user groups for each protocols, e.g. apache(web server), and configure file and directory access control using ACL or a similar effective mechanism for each users in these groups. Access permissions and ACL shall be reviewed periodically.
CR-2.1 RE(1)	CompletedAdded acl package	TC_CR2.1_1	Default Action
CR-2.1 RE(2)	CompletedAdded acl package	TC_CR2.1_1	Default Action
CR-2.1 RE(3)	CompletedAdded sudo package	TC_CR2.1_1	Default ActionSince the privileges/supervisor overrides are application specific, this requirement must be implemented at application level
CR-2.1 RE(4)	N.A.	None	This is for SL-4

Req ID	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
CR-2.2	N.A.	None	This requirement can not be supported by CIP. However, CIP has following recommendations for meeting this require-ment**SYSTEM**:1. Every interface needs to use pam or similar authentication2. Network control on a system level needs to adhere to security best practices**APP**:1. Support the ability to disable SSID broadcast function2. Support client white-list function3. Support alarm on known vulnerable encryption (e.g., WEP)4. Record client connection events5. Support ACL integration6. Application should not use vulnerable protocols underneath
CR-2.3	N.A.	None	There is no component level
SAR-2.4	N.A.	None	This requirement only applies to Software
SAR-2.4 RE(1)	N.A.	None	This requirement only applies to Software Applications
EDR-2.4	N.A.	None	This requirement is not supported by CIP.Embedded devices only need to support this requirement if they utilize mobile code technologies such as Java, USB ports (autorun)
EDR-2.4 RE(1)	N.A.	None	Same as EDR-2.4
HDR-2.4	N.A.	None	It’s for host devices
HDR-2.4 RE(1)	N.A.	None	It’s for host devices
NDR-2.4	N.A.	None	It’s not applicable to CIP same as EDR-2.4

Req ID	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
NDR-2.4 RE(1)	N.A.	None	It's not applicable to CIP same as EDR-2.4
CR-2.5	CompletedAdded package openssh	None	CIP added openssh package to meet this requirement.However, it's application developer's responsibility to configure timeout period for the session as well as terminating the session after timeout.This can be implemented in many ways hence it's left to CIP users.
CR-2.6	CompletedAdded package openssh	None	Same as CR-2.5
CR-2.7	Completed Added pam and openssh package	None	Same as CR-2.5
CR-2.8	CompletedAdded package auditd	None	This requirement is supported by CIP.However, application needs to configure applicable types of events for audit, all such events should be recorded which should be made available
CR-2.9	None	This requirement is supported by CIP.However, application needs to configure log storage capacity, and when logs should be discarded after reaching certain configured storage limit.	
CR-2.9 RE(1)	CompletedAdded package auditd and rsyslog	TC_CR2.9-RE1_1	Same as CR-2.9

Req ID	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
CR-2.10	In-progress	TC_CR2.10_1	CIP supports this requirement by adding packages auditd and rsyslog.Applications need to harness capabilities of these packages and demonstrate to meet this requirement.
CR-2.11	CompletedAdded package chrony	TC_CR2.11_1	Default Action
CR-2.11 RE(1)	CompletedAdded package chrony	TC_CR2.11_1	CIP supports this requirement by chrony package.However, application needs to configure logs in such a way that logs are generated with system time synchronized
CR-2.11 RE(2)	N.A.	None	This is for SL-4
CR-2.12	CompletedAdded packages audits and syslog-ng	TC_CR2.12_1	Default Action
CR-2.12 RE(1)	N.A.	None	This is for SL-4

Req ID	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
EDR-2.13	N.A.	None	SYSTEM and HW: Physical diagnostic and test interfaces need to be protected from unauthorized access, if they provide the ability to execute commands on the system, affect its core functionality or read out non public data. Protection could be done by physical access restriction and/or an authorization method similar to the productive authorization methods described in this document. The Level of protection needed has to be assessed via a threat and risk analysis. Also, it needs to carefully consider the necessity of installing test interfaces. In particular, it is desirable to remove the JTAG interface in the final production because it may cause unexpected behavior for even supplier due to non-public instructions to the processor for hardware debugging.

Req ID	Status if supported by CIP	IEC-62443-4-2 tests reference	CIP recommendation
EDR-2.13 RE(1)	CompletedAdded packages syslog-ng, auditd	TC_CR2.12_1	CIP supports this requirement by adding required packages.In order to meet this requirement application needs to do logging when diagnostic and test interfaces are accessed. All such interfaces should be considered as part of application or system threat model. If there are some interfaces which are used only during design and development , such interfaces should be removed before devices are shipped out.
HDR-2.13	N.A.	None	This requirement is for host devices
HDR-2.13 RE(1)	N.A.	None	Same as HDR-2.13