#

CIP Security Requirements

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2021-02-24	Draft security requirement based on IEC-62443-4-x created	Dinesh Kumar	TBD

Overview

This document is intended to capture CIP security requirements based on IEC-62443-4-2 standard. In future this document should be revised based on additional security requirements.

IEC-62443-4-2 Requirements

Following table outlines CIP security requirements. These requirements are derived from IEC-62443-4-2 security requirements which could be applicable to CIP.

Each requirement has been assigned one unique identifier as requirement ID e.g. CIP_SEC_IEC_FUNC_REQ_1 which can be interpreted as _

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_FUNC_REQ_1	Support human user identification & authentication, user account management, password management	Following are the key requirements1. System should support identification and authentication for all users at all accessible interfaces, either locally or by integration into a system.2. System should be able to uniquely identify and authenticate all human users3. System should support account management functions in order to make changes such as activate, modify, disable and remove user accounts4. System should support default authenticator change5. System should support changing password once expired	IEC-62443-4-2 CR1.1, CR1.1(1), CR1.3, CR1.5, CR1.7(1), CR1.7(2)

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_FUNC_REQ_2	Limit number of unsuccessful login attempts, limit on concurrent sessions	1. System should have provision to limit number of unsuccessful login attempts and once unsuccessful login attempts exceed, the account should be locked either temporarily for some time or permanently and admin user should be able to unlock it.2. System should limit number of concurrent sessions from any user(human, process or device) to prevent DoS attack	IEC-62443-4-2 CR1.11, CR2.7
CIP_SEC_IEC_FUNC_REQ_3	Multifactor authentication for all interfaces for human users	System should provide multifactor authentication for human users on all interfaces	IEC-62443-4-2 CR1.1(2)
CIP_SEC_IEC_FUNC_REQ_4	Unique identifiers for identifying each account	System should provide capability to integrate into a system that supports function of generating unique identifiers	IEC-62443-4-2 CR1.5(1), CR1.9(1), CR1.14(1)

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_FUNC_REQ_5	Capability to access secure storage for cryptographic keys/authenticators	System should provide capability to access secure hardware or TPM to meet following requirements1. Access authenticators stored in secure HW2. Symmetric keys stored in secure HW3. Private keys stored in secure HW	IEC-62443-4-2 CR1.5(1), CR1.9(1), CR1.14(1)
CIP_SEC_IEC_FUNC_REQ_6	PKI (Public Key Infrastructure) support, use of cryptography	System should support following functionality 1. Usage of PKI for authentication2. Authenticator feedback3. Strong symmetric key based authentication4. All communication protected by integrity and authentication5. Information confidentiality by applying encryption6. Key management according to NIST SP 800-577. Usage of cryptographic algorithms recognized by international standards	IEC-62443-4-2 CR1.8, CR1.9, CR1.10, CR1.14, CR3.1, CR3.1(1), CR3.4, CR3.4(1), CR4.1, CR4.3

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_FUNC_REQ_7	Authorization enforcement support	System should support following functionality1. Authorization enforcement for all authenticated and identified users2. Usage of control policies like identity based policies, role based policies and rule based policies	IEC-62443-4-2 CR2.1, CR2.1(1), CR2.1(2), CR3.9
CIP_SEC_IEC_FUNC_REQ_8	Protection of audit information	System should support protection of audit information, audit logs and all the audit tools from unauthorized access, modifications, deletions	IEC-62443-4-2 CR3.9
CIP_SEC_IEC_FUNC_REQ_9	Supervisor override	System should support functionality to temporarily elevate privileges of a normal user to higher level, this should be recorded and controllable	IEC-62443-4-2 CR2.1(3)

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_FUNC_REQ_10	Session locking, remote session termination	System should provide following functionality in order to protect user sessions1. Unattended open sessions should get locked after a configurable time period and either user or admin should be able to unlock2. Terminate remote session after configurable period of time	IEC-62443-4-2 CR2.5, CR2.6
CIP_SEC_IEC_FUNC_REQ_11	Auditable events	System should support following functionality for auditable events1. Create audit records for security events such as access control, request errors, control system events, backup-restore events, configuration changes, audit log events2. Each record should have timestamp, source, event id, event results3. Automated notification of integrity violation	IEC-62443-4-2 CR2.8, CR2.10, CR2.12, CR2.12(1)

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_FUNC_REQ_12	Audit storage	System should support following functionality for audit storage1. Allocate audit record storage according to recommended size2. Mechanism to protect against failure of component when it reaches audit storage limit3. Give warning when audit record storage capacity threshold reached	IEC-62443-4-2 CR2.9, CR2.9(1)
CIP_SEC_IEC_FUNC_REQ_13	Software and information integrity	System should provide following functionality to support this requirement1. Capability to detect authenticity of software and information2. Report integrity violations in an automated fashion	IEC-62443-4-2 CR3.4(1), CR3.4(2)
CIP_SEC_IEC_FUNC_REQ_14	Denial of service protection	System should support mitigation for DoS attacks and make sure essential services are kept intact	IEC-62443-4-2 CR7.1(1)

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_FUNC_REQ_15	Control system backup and recovery	System should support following functions1. Capability to support system level backup including system and user state without affecting normal operation2. Backup information should be encrypted in order to safeguard it, backup information should not store encryption keys instead encryption keys should be backed up separately3. The integrity check of back up data should be supported	IEC-62443-4-2 CR7.3, CR7.3(1)

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_TIMESYNC_REQ_16	Time synchronization	System should support following functions1. Capability to create timestamps that can be used in logs, audit records and other required places2. Timestamps are synchronized system wide with a common source3. Time synchronization mechanism should be protected in such a way that any alteration could be detected	IEC-62443-4-2 CR2.11, CR2.11(1)

Other Security Requirements

File Integrity

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_NONFUNCTIONAL_REQ_1	Integrity of source code, scripts, executable	Receiver of CIP shall be able to verify integrity of scripts, source code and executable	IEC-62443-4-1 SM-6

Development Environment Security

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_NONFUNC_REQ_2	Development environment security	There shall be a process to ensure protection of product during, development, production and delivery including software updates during design, implementation, testing and release	IEC-62443-4-1 SM-7

Private Key Protection

Requirement ID	Requirement	Description	Source of requirement
CIP_SEC_IEC_NONFUNC_REQ_3	Protection of private keys	There shall be a process to protect all private keys used for code signing from unauthorized access or modifications	IEC-62443-4-1 SM-8

CIP Core CVE Tracking

CIP_SEC_IEC_NONFUNC_REQ_4

CIP Core should define and implement CVE tracking methods to incorporate latest fixes for CVEs

CIP Kernel CVE Tracking

CIP_SEC_IEC_NONFUNC_REQ_5

CIP Kernel should define and implement CVE tracking methods to incorporate latest fixes for CVEs

Security Level

CIP_SEC_IEC_NONFUNC_REQ_6

CIP targets to achieve SL-3 by adding required security features and configurations. However, it depends upon final recommendation from Certification Body, what could be the Security Level.

Security Updates

CIP_SEC_IEC_NONFUNC_REQ_7

CIP should apply latest security fixes published through CVEs.

Default User Accounts

CIP_SEC_IEC_NONFUNC_REQ_8

CIP should publish default user accounts and their privileges.

Security Context

CIP_SEC_IEC_NONFUNC_REQ_9

Product owners should define product security context as expected in IEC-62443-4-1 SR-1.