#

IEC 62443-4-2 App & HW Guidelines

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2021-09-30	Draft IEC 62443-4-2 APP & HW guidelines document	Dinesh Kumar	To be reviewed by CIP Security WG members
002	2022-01-28	Updated all sections	Dinesh Kumar	To be reviewed by CIP Security WG members
003	2022-03-29	Added reference for CR4.3, updates for unique identification and authentication	Dinesh Kumar	To be reviewed by CIP Security WG
004	2022-04-22	Added reference for IEC-62443-4-2 tests	Dinesh Kumar	To be reviewed by CIP Security WG
005	2022-07-24	Fixed SWG comments	Dinesh Kumar	
006	2023-01-4	Updated table based on exida gap assessment summary	Dinesh Kumar	To be reviewed by CIP SWG

1. Objective

The primary objective of this document is to provide guidelines to CIP users for meeting IEC-62443-4-2 security requirements. The document explains about each IEC-62443-4-2 requirements whether it has already been met by CIP.

This document has been prepared based on the extensive consultation with exida, Certification Body (*CB) as part of CIP IEC-62443-4-2 Gap Assessment.

In addition this document also explains about iec security layer added in CIP to meet IEC-62443-4-2 security requirements.

2. Acronyms

Acronym	Meaning
CB	Certification Body such as exida
CIP	Civil Infrastructure Platform
CIP Users	CIP based product owner
FR	Foundational requirements from IEC-62443-4-2

3. Assumptions

Assumption	Impact
This document would be used as guideline document to meet final IEC-62443-4-2 security requirements by CIP users	Following this document as it is may impact end product security strength

4. Scope

This document covers IEC-62443-4-2 guidelines from IEC-62443-4-2 Gap Assessment with exida. As some of the IEC-62443-4-2 requirements are met by CIP and others are not met by CIP. IEC-62443-4-2 security requirements which are not met by CIP should be met by CIP end products.

Detailed gap assessment document can be found at CIP IEC-62443 Gap Assessment ## 5. IEC-62443-4-2 CIP Guidelines

This section provides information about each IEC-62443-4-2 requirements whether it's met by CIP, or is not met by CIP. Some requirements need additional hardware support which should be met by CIP end products.

Columns provide following information in the tables of each section.

Req ID

This requirement id is same as in IEC-62443-4-2.

Requirement name

Brief name of IEC requirements

Requirement description

Simplified description of IEC-62443-4-2 requirements.

Supported by CIP

TRUE: Indicates

Requirement is fully supported by CIP and CIP users don't need to do anything for meeting the requirement, just utilize the capability provided by CIP.

FALSE: Indicates * CIP does not support the requirement or it's partially supported by CIP * It requires HW solution

Need application support

TRUE: Indicates CIP does not alone meet this requirement and some additional support from CIP user application is needed.

FALSE: Indicates no application support is needed.

Need HW solution

TRUE: Indicates the requirement needs hardware support

FALSE: Indicates no hardware support needed to meet the requirement

CIP Recommendation

CIP members did extensive investigation of IEC-62443-4-2 standard and had discussion with Certification Body. The recommendations are based on the discussion with Certification Body.

Default Action

Here default action means use CIP provided package or equivalent to meet the requirement. Even though CIP as platform provides several packages, CIP users need to re-use capabilities provided by the packages to meet specific security requirements.

5.1 FR-1 Identification and authentication control

The details of each requirement of this section can be found in FR-1 document

5.2 FR-2 Use Control

The details of each requirement of this section can be found in FR-2 document

5.3 FR-3 System Integrity

The details of each requirement of this section can be found in FR-3 document

5.4 FR-4 Data Confidentiality

The details of each requirement of this section can be found in FR-4 document

5.5 FR-5 Restricted Data Flow

The details of each requirement of this section can be found in FR-5 document

5.6 FR-6 Timely Response to Events

The details of each requirement of this section can be found in FR-6 document

5.7 FR-7 Resource Availability

The details of each requirement of this section can be found in FR-7 document

6. CIP Security packages

All the security packages added in isar-cip-core can be found at CIP Security images

In addition section 5 of this document has reference to all packages along with the security requirements.

7. IEC Security Layer

CIP developer extensively investigated IEC-62443-4-2 security requirements and available Debian packages to meet the IEC requirements.

These packages form IEC security layer in CIP.

7.1 Running security tests

IEC security tests can be executed by following the steps specified at CIP Security Tests gitlab

7.2 Adding security package

Adding security packages to isar-cip-core has two steps.

Step-1

Create a package proposal (PDP process)with the required details of the package which needs to be added and send it for CIP Core WG review and approval. Once approval is completed, the package can be added to the isar-cip-core gitlab repository

Step-2

Add package to isar-cip-core (isar-cip-core git lab repo) repositery and send the MR for review and approval.

7.3 Adding security test

TBD