#

User Security Manual

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2021-09-30	Draft User Security Manual	Dinesh Kumar	To be reviewed by CIP Security WG members
002	2022-05-30	Fixed SWG review comments in gitlab	Dinesh Kumar	CIP SWG

1. Objective

This document contains items identified during IEC-62443-4-1 and IEC-62443-4-2 Gap Assessment for user security manual. It should contain following items and is subject to revision based on Certification Body feedback or any other inputs from other CIP members.

- How to operate CIP in secure manner
- CIP security configurations
- CIP users privileges to operate or configure the end products

This document is subject to revisions based on new findings or investigations in future.

2. Assumptions

Assumption	Impact
All documented guidelines are strictly followed by CIP users	These are recommendations identified from IEC-62443-4-2 & IEC-62443-4-1 investigation, not following these guidelines indicate non compliance of the product to IEC.

3. Scope

This document covers requirements from IEC-62443-4-1 & IEC-62443-4-2, where we have received gap assessment comments from Certification Body.

4. Guidelines

4.1 IEC-62443-4-2 (EDR-3.2) Protection from malicious code

CIP platform does not meet this requirement completely hence CIP users are advised to do risk assessment for the end product and find out suitable means to deploy for mitigating the risk by installing malicious code on the device. Some of the important areas to consider for protection includes.

- USB host access
- Detect integrity violation of application binaries and data files

Depending upon the end product various techniques can be adopted e.g. no execute bit (NX), data execution prevention (EDP), address space layout randomization (ASLR), stack corruption detection etc.

4.2 IEC-62443-4-2 (NDR-3.2) Protection from malicious code

CIP platform does not support this requirement and hence CIP user should consider the use of white listing or signing the software binaries in order to meet this requirement.

Other options could be to use suitable IPS/IDS packages provided by CIP platform.

4.2 IEC-62443-4-2 (CR-7.1) Denial of service protection

CIP platform meets this requirement by providing several security packages for ensuring device security. However, denial of service protection is very wide and requires measures to be taken by CIP end users as well.

CIP users should do CRT(Communication Robustness Testing) testing on end devices to conform device meets robustness testing requirements.

pam, openssh and acl packages can help to achieve Denial of service protection.

4.3 IEC-62443-4-2 (CR-7.3) Control System Backup

CIP members are investigating to include suitable package which can support this requirement. However, CIP users need to configure data which need to be taken as remote backup.

In addition to taking backup CIP users should also check and confirm data can be restored on regular basis.

4.4 IEC-62443-4-2 (CR-6.2) Continuous Monitoring

CIP provides capabilities to monitor system continuously. CIP provides packages like aide, syslog-ng which can be configured to monitor system continuously depending upon the use case.

For more information, refer other related documents.

5. CIP System Monitoring

CIP as platform provides various techniques for system monitoring. However, it is left to CIP users to select appropriate methods for their use cases. e.g. aide, syslog-ng, auditd are some of the examples.

Various logs to monitor are > /var/log/syslog > /var/log/auth.log > /var/log/boot.log > /var/log/dmesg > /var/log/faillog