CIP Requirements

Table of contents

Revision History

Revision No	Date	Change description	Author	Reviewed by
001	2023-01-04	Template document for CIP requirements	Sai Ashrith	Dinesh Kumar
002	2023-03-08	Add CIP functional and non-functional requirements	Dinesh Kumar	

Introduction

This document is intended to define and document CIP requirements as a platform.There are generic CIP platform requirements which are mainly derived from CIP white paper.

IEC-62443-4-1 SM-1 expects the component to have defined requirements which can be tested. The requirements can be functional, non-functional, performance, security etc.

The basic goals of CIP have been documented in a whitepaper available at CIP project portal. According to the Certification Body the goals defined in the CIP whitepaper are quite abstract and cannot be considered to meet IEC-62443-4-1 Secure Development Process requirement.

CIP Functional Requirements

S No.	Requirements	Details	Responsible WG
1	Re-use Linux mainline kernel, customise configs based on CIP members requirement	CIP to reuse Linux mainline kernel	CIP Kernel
2	Provide CIP RT kernel by applying PRE-EMPT_RT patches	CIP to maintain its own RT kernel	CIP Kernel
3	Develop meta-data to create minimal CIP reference images	Create recipes and meta-data to re-use Debian packages for creating minimal CIP reference image	CIP Core
4	Support multiple cpu architectures in CIP reference images	Recipes and meta-data should be configurable to support multiple architectures such as amd64, arm64, armhf	CIP Core, CIP Kernel
5	Support Secure boot	Support secure boot with or without secure storage	CIP Core, CIP Kernel
6	Support SWUpdate with local file and OTA	CIP users should be able to update devices using local file using sdcard or eMMC or using OTA updates	CIP SWUpdate
7	Support SWUpdate with signed & encrypted images	CIP should support SWUpdate with Signed and Encrypted images	CIP SWUpdate

S No.	Requirements	Details	Responsible WG
8	CIP Security detailed requirements are documented in a separate document at	https://gitlab.com/cip-project/cip-documents/-/blob/master/security/security_requirements.md	CIP SWG & CIP Core
9	Deliver a generatable SBOM along with the sample configuration	The CIP packages, the tooling to create the packages and system image for the reference hardware shall be enabled to also provide a SBOM for the provided software	CIP Core, CIP Kernel, CIP SWUpdate

CIP Non-Functional Requirements

S No.	Requirements	Details	Responsible WG
1	Follow upstream first policy for CIP Core and CIP Kernel development	CIP members to follow upstream policy for the issue fixes in CIP Kernel or CIP Core should be first upstreamed before accepting in CIP	CIP Kernel
2	Maintain SLTS kernel for 10+ years	CIP members to decide democratically SLTS kernel and maintain for up to 10 years by providing security fixes and updates to CIP users	CIP Kernel
3	Use Debian based packages or third party applications to create CIP Core reference images	The primary source of CIP Core packages is Debian repositories. However, some packages may also come from other repositories based on all members decision	CIP Core
4	Accept only kernel patches which are upstreamed	CIP Kernel maintainers to ensure all the patches applied in the CIP kernel are from stable upstream trees	CIP Kernel