CIVIL INFRASTRUCTURE PLATFORM

CIP Technical Steering Committee Meeting

Date: 7th December 2021.

Roll Call

TSC members (Alphabetical order by company name)

Attendees (Please change to **Bold**, if you attend this meeting) (Key shortcut: Ctrl+b)

Company	Members
Codethink	Sam Wilson (Representative)
Cybertrust	**Hirotaka Motai (Representative)**
Hitachi	**Hidehiro Kawai (Representative)** Takuo Koguchi
IoT.bzh	Stéphane Desneux (Representative)
Linutronix	Jan Altenberg (Representative)
Moxa	Jimmy Chen (Representative)
Plat'Home	**Masato Minda (Representative)**
Renesas	**Chris Paterson (CIP Testing WG Chair)** Kento Yoshida Kazuhiro Fujita **Takehisa Katayama (Representative) (Voting)**
Siemens	Jan Kiszka (Representative) (Kernel Team Chair) Wolfgang Mauerer (Representative) (Voting) Urs Gleim **Yasin Demirci (Security WG Chair)**
Toshiba	**Dinesh Kumar** **Daniel Sangorrin** **Kazuhiro Hayashi (Voting Representative) (CIP Core / Software Update Chair)** Venkata Pyla **Nobuhiro Iwamatsu (Kernel Maintainer)**

	Punit Agrawal Shivanand Kunijadar **Yoshi Kobayashi (Representative) - Chair**
VES Solutions	Fred Night **Josiah Holder**
Denx	**Pavel Machek (Kernel Maintainer)**
	Ulrich Hecht (Kernel Developer)
Linux Foundation	**Neal Caidin**

Discussions

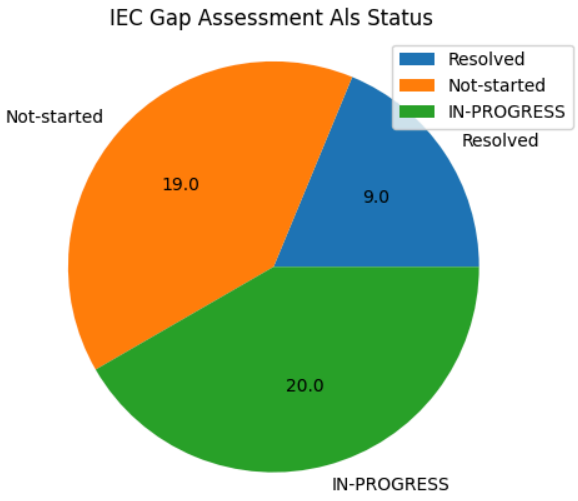
Security Working Group

Items need to be approved by TSC voting members

- Motion by SWG: Gitlab permission process: https://gitlab.com/cip-project/cip-documents/-/blob/master/security/development_environment_security.md#6-policy-for-cip-repository-maintainer-privilege
    - Action(Yasin): Ask for vote to TSC members by email.

Status updates

- Progress for supporting AIs:
    - AI Lists: CIP_AI_From_4-1_Gap_Assessment
    - Status: https://gitlab.com/cip-project/cip-security/iec_62443-4-x/-/issues
    - Following is the status of IEC-62443-4-1 & IEC-62443-4-2 AIs



    - CIP Security WG members tasks status
        - Toshiba Total = 16 (In-progress: 7, Resolved: 7, Released: 2)
        - Renesas Total = 8 (In-progress: 8, Resolved: 0)
        - Siemens Total = 4 (In-progress: 4, Resolved: 0)
        - Moxa Total = 1 (In-progress: 1, Resolved: 0)
- **Survey for 62443 in member companies**
    - Discussion: Neal recommended to not ask on specific certification target dates for 62443-4-2 due to antitrust regulations.
        - Neal proposed an alternative question, the query will be resend. (Al Yasin)
- **Roles and responsibilities**
    - Discussion: https://gitlab.com/cip-project/cip-security/iec_62443-4-x/-/issues/9
    - Proposal (in discussion): https://docs.google.com/presentation/d/1eNx7cvi5dskTBxlbWOSe6f7RA6T7Hk99/edit#slide=id.p3
    - Question: What are current policies regarding Gitlab admins and maintainers? Context: Security WG wants to restrict people becoming admins/maintainers.
    - SWG reevaluated: Big changes are not needed right now to fulfill the IEC 62443. We propose this yearly process for maintainer rights only:
        - https://gitlab.com/cip-project/cip-documents/-/blob/master/security/development_environment_security.md#6-policy-for-cip-repository-maintainer-privilege
- **CIP AWS access**
    - How are our AWS instances managed? Who has access? How do users authenticate?
- **First biweekly working meeting was held**
    - ~1:15h
    - The focus on working tasks seemed to work well.

Kernel Team Working Group

Items need to be approved by TSC voting members

- **none**

Status updates

- **CIP IRC weekly meeting**
    - logs
        - Dec 2nd
- **CIP kernel release**
    - 4.4
        - none
    - 4.19
        - v4.19.217-cip62 on Dec 1st by Iwamatsu
        - v4.19.217-cip62-rt23 on Dec 1st by Pavel
    - 5.10

        - v5.10.83-cip1 on Dec 5th by Iwamatsu
-

CIP Core Working Group

Items need to be approved by TSC voting members

- None

Past minutes

- past meetings

Debian Extended LTS

- Current plan (confirmed by TSC): CIP will fund **1,530 EUR / 6 months**
    - **425 EUR**: Cost for Debian 8 package maintenance
        - "Priority: Required" and their dependencies + CIP's requests (busybox, binutils, openssl, openssh)
    - Remaining(1,105 EUR): Used to improve infrastructure of Debian (ELTS)
- AI(Kazu): Package proposal for Debian jessie
    - WIP: Create "pkglist_jessie.yml" like buster then send the proposal

CIP Core Testing

- Some improvements in image deployment (See isar-cip-core section)
- WIP: How to integrate IEC tests

IEC-62443-4-1 requirements

- Suspended: Plan of Security WG about package proposal
    - Waiting for the conclusion of the target Debian version in security WG
- CIP Core release image and release process
    - Clarifying detailed requirements and concrete tasks
- Debian repository for CIP Core
    - Clarifying detailed requirements and concrete tasks
- Bug tracking system in CIP
    - Start by doing some simulations with some examples of security issues

Reproducible builds

- WIP: will create a patch in isar to remove the `/var/cache/debconf/config.dat` file and this can be created in the next boot

Updates to Isar-cip-core

- Updates (master)
    - start-qemu.sh: Add defaults for IMAGE_SECURITY
    - Improve deployment: Performance, branch handling, permission settings
    - Squashfs and dm-verity supports

        - Add new class to create a squashfs based root file system
        - Add verity-img.bbclass for dm-verity based rootfs
        - Create a initrd with support for dm-verity
        - Create an read-only rootfs with dm-verity
    - Adjustments for read-only rootfs
    - linux-cip: Update to latest releases
- Updates (next)
    - Add kas option to selection 4.19 explicitly
    - **linux-cip: Add recipe, option file and menu entry for 5.10.83-cip1**
        - Next: Use 5.10.y-cip kernel for bullseye images in CI
- WIP: Updating kernel configs for BBB
    - Discussions: #1 #2
    - The latest (v2) patch for cip-kernel-config is now in the development branch
    - TODO: Test the updated configs with BBB

Tools

- cip-core-sec
    - It seems that some codes are Debian 10 specific
    - AI: Make the tool available with Debian 11

CIP Testing Working Group

Items need to be approved by TSC voting members

- None

Status updates

- Fixed GitLab runner network issues.
- Currently working on adding support to use the latest isar-cip-core for Kernel testing.

Discussions

- None

Software Update Working Group

Items need to be approved by TSC voting members

- None

Status updates

- Replacing BBB kernel config: Status and AIs
    - (Same as “Updating kernel configs for BBB” in isar-cip-core above)
- (RESEND) [isar-cip-core] Read-only root file system with dm-verity => Applied to “next”

> *This patch series adds support for a read-only squashfs based root

filesystem
wit SWUpdate support and secureboot.

The build is somewhat complex as we need the output of dm-verity to generate
the initramfs. The build is split in the following steps
1. Build the root file system
2. Generate a squashfs image - this can also be replace by another image format(e.g. ext4)
3. Build from the image the dm-verity partition and add it to the end of the image
4. Add the resulting verity environment to the initrd
5. Build the signed efi tool chain.

This series needs SWUpdate 2021.11. The necessary changes are currently backported.

- Testing SWUpdate in CIP
    - AI: Create an issue to collect information for testing
        - Create README that includes basic instruction for testing
        - Share the common configurations, etc.