CIVIL INFRASTRUCTURE PLATFORM

CIP Core regular meeting

- **Date: June 6th (Tuesday), 2023**
- Time: Tokyo (Japan) JST 17:30 (30min~1h)
    - **Please check your local time in timeanddate.com**
- Zoom
    - Meeting URL
    - Dial-in numbers
    - Meeting ID: 917 9128 4612
    - Passcode: 248841
- Past meetings

Rules

- http://www.linuxfoundation.org/antitrust-policy
- Please mark with (PRIVATE) those parts that should not appear in the public version of these minutes

Roll Call

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

Company	Members
Bosch	Philipp Ahmann Sietze van Buuren
Cybertrust	**Hiraku Toyooka** Alice Ferrazzi
Hitachi	
Linutronix	
Moxa	**Jimmy Chen**
Plat'Home	**Masato Minda**
Renesas	Chris Paterson Kento Yoshida Kazuhiro Fujita Hung Tran

	Nhan Nguyen
Siemens	**Jan Kiszka** Christian Storm Raphael Lisicki
Toshiba	**Kazuhiro Hayashi (WG chair)** Dinesh Kumar **Venkata Pyla** **Sai Ashrith** Shivanand Kunijadar Tho Nguyen Dat

Discussion

Action items updates

- AI(Kazu): Update WG wiki page
- Debian Extended LTS
  - **AI(Renesas): Share the package proposal**
    - [04/25] Proposal creation in progress, yet to be shared in ML
    - [05/23] No update
  - AI(Kazu): Package proposal for Debian jessie
    - WIP: Creating the proposal
      - ... but LTS defines the format of package list. It might be better to revise cip-pkglist scripts to meet the format
- IEC-62443-4-1
  - AI(Kazu): Create the package proposal for bullseye minimal packages
    - WIP: Creating the proposal
- CIP Core testing
  - **AI(Plat'Home): Update kernel configs for OpenBlocks IoT**
    - Apply the required changes to 4.19 kernel config (Check with Iwamatsu-san)
    - (2023-06-06) Now I'm preparing the kernel configuration while consulting with Iwamatsu-san. I should be able to send a merge request by tomorrow.
- cip-core-sec
  - AI(Toshiba): Add improvements to solve some issues and make the project official (move to cip-project)
  - AI(Toshiba): Update the ISAR gitlab-ci integration branch
- IEC 62443-4
  - Supporting secure storage on Renesas RZ/G2M

        - **AI(Kent): Confirm if NDA is required or not (maybe not required)**
            - [04/25] No update
            - [05/09] No update
            - [05/23] Kent-san has not done confirming this yet, but he will share the result soon.
            - 6/6 No Renesas member join

Debian LTS / Extended LTS

- The query from Freexian (Thorsten): Debian 10 buster package list
    - Kazu sent the CIP package list for Debian 10 to Freexian (March 31st)
    - Renesas is requesting to add some packages
        - AI(Renesas): Share the package proposal
- AI(Kazu): Package proposal for Debian jessie

IEC-62443-4

- **CIP IEC-62443 certification activities**
    - Prepare for next BV meeting (06/15)
        - SWG members updating IEC-62443-4-1 BV checklist for compliance
    - Create private gitlab repository for sharing with BV and to be used for tracking IEC assessment action items and issues
        - Requested Kent to create the repository, waiting for his response
- **Confirm TPM based secure storage support in isar-cip-core**
    - From last meeting discussion, we are tracking this support in the following issue
        - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/63
        - TPM support has been confirmed on QEMU x86 and QEMU arm64 based on the
            - We have verified by changing swtpm file which has encryption keys, if swtpm file is changed, booting fails
            - **Is there any other way to verify? If we want to put this as test case in IEC layer?**
        - Identifying tests for confirming TPM and data encryption at rest support based on ISASecure CSA-311 document in progress
- **Supporting isar-cip-core images based on Debian 12 from IEC-62443 standpoint**
    - As soon Debian 12 support will be enabled in isar-cip-core and CIP Kernel 6.1 might be supported as well, so shall we consider using Debian 12 based images for CIP IEC evaluation? Just wanted to check opinions from all members
    - [04/25]

        - Continue to discuss the pros and cons, specially understanding how much time it may take for CIP kernel 6.1 support in CIP
        - Jan: Someone in SWG should check with the latest Debian 12 and kernel 6.1 whether IEC tests can pass or there are some issues
    - [05/09] Image build fails, Issue reported in isar-cip-core https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/64
    - [05/23] Image without security extension is booted. However, Security image requires changes for pam_passwdqc.
    - **[06/06] "pam_cracklib" is deprecated in bookworm, so as an alternative "pam_passwdqc" will replace it from bookworm onwards, SWG will share the patch for this change.**
- Confirming IEC layer tests on QEMU arm64 & armhf for bullseye and kernel 5.10
    - All related changes are merged for both arm64 and armhf
- **Supporting SWUpdate and Secure boot on Renesas RZ/G2M**
    - [05/23] Renesas: patch to support SWUpdate for G2M has been sent. Renesas is checking on SB.
    - [6/6] The patch to enable SWUpdate is merged
    - Kazu would like to check how the changes are tested
- Supporting secure storage on Renesas RZ/G2M
    - Q: If CIP members (non Renesas members) want to use / evaluate secure storage features on G2M, does the member need NDA?
        - AI(Kent): Confirm if NDA is required or not (maybe not required)
        - If not required, we can check more details about drivers below as the next step
- AI(Kazu): Create the package proposal for bullseye minimal packages
- CIP Core release
    - When: See "versioning rule" below
    - What:
        - Recipes
        - Test results
        - Security reports (by cip-core-sec)
        - Note: Releases don't include CIP Core images
    - Versioning rule: Semantic versioning style: x.y.z
        - x : All other significant changes than y and z
        - y : Incremented for each Debian point release
        - z : Incremented only when critical bugs are fixed
    - **Remaining questions:**
        - After stable (oldstable, LTS, ...), when should CIP Core create release (when increment "y")?
        - AI (SWG)[05/09]: Investigate current isar-cip-core KAS menu option and create table for supported Debian versions and meta-data versions
- Recent releases
        - v1.0-rc1

        - V1.0

Reproducible builds

- Open issues
    - #54 [Software update image is not reproducible] - Open
        - (An image that includes SWUpdate package and related settings)
        - Sent patch to fix this issue in ISAR
        - Sent patch in isar-cip-core to get the feedback.
        - **Applied**
    - #56 [vmlinux is not reproducibly built in arm[,64] architectures] - Open
        - Reported issue in upstream (ISAR)
        - Sent patch in upstream isar to fix this issue.
        - **Applied** to isar master branch
        - Need to update isar reference commit in isar-cip-core
    - #58 Diffoscope tool could not verify disk images with partitions - Open
        - Sent query in reproducible-build community
        - Diffoscope doesn't support disk image comparison with partition table in it, created issue in diffoscope project.
        - Next action: use individual file system images like ext4 and verify if they are bit by bit identical
            - Received feedback from Jan regarding the patch to include ext4 filesystem in the build
            - Checking how to extract the file system images from the wic image file using kpartx.

isar-cip-core

- Repositories & mailing list
    - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/commits/master/
    - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/tree/next
    - https://lore.kernel.org/cip-dev/
- **Updates**
    - swupdate: Enable SWUpdate for RZG2M
    - scripts: Add script to test different artifacts in the image are bit identical
        - And use it for CI
    - Update software versions
        - Kas 3.2.3
        - CIP kernel / kernel config : Latest
    - Other fixes, improvements for scripts, docs, etc.
- Releases
    - None
    - **Kazu: Any plans for v1.1 release?**
        - Debian 11.7 released

        - Jan: No, will make release around end of July (quarterly)

deby

- (No update)

CIP Core Testing

- deby has the copy of linux-cip-ci's LAVA functions
    - (No update)
    - Plan: Create a separated repository to provide the LAVA functions => Other projects like linux-cip-ci, deby (and isar-cip-core?) reuse the repository
    - Created the draft project in playground
    - Implemented the draft and validating
- No OpenBlocks IoT device available in LAVA
    - The recipes for the device have been implemented in development branch and the OS images (kernel & rootfs) are built by CI
    - **AI(Plat'Home): Update kernel configs**
        - Solved once the required changes for kernel config are merged
    - **Next step:**
        - 0: Confirm that the devices are enabled in LAVA (already enabled)
        - 1: Create recipes for the device in isar-cip-core/deby (if not)
        - 2: Test the kernel+rootfs by CI
            - deby : Test with LAVA
            - isar-cip-core : Test with KernelCI?
- **CIP Core to test CIP kernel**
    - Query from Chris in ML: "If we have multiple versions of cip-core - which do we use for kernel testing?"
        - What does the "multiple versions" mean here?
            - Debian version? (e.g. bullseye)
            - isar-cip-core version? (e.g. v1.0)
            - Flavor of images? (e.g. minimum, security, ...)
        - Any conclusion about this discussion?
        - [05/23] According to Chris as of now main focus of CIP testing is kernel testing so whatever flavor of isar-cip-core image is taken for testing, it does not matter much because kernel remains same
    - Kazu: Shall we check (again) the version combinations of kernel & Debian for CIP kernel / Core testing?
        - The (old) information that was agreed by TSC (several years ago...)

Kernel	Debian	Note
4.4	8 (jessie)	isar-cip-core does not provide jessie, need to use buster instead?

4.19	10 (buster)	
5.10	11 (bullseye)	
6.1	12 (bookworm)	

        - Any discussions / conclusions in kernel WG?
            - [04/25] Jan: This combination looks more logical, same should continue
            - [05/09] Requested a discussion with Chris for consolidating and preparing for IEC documentation
            - [05/23] Had meeting with Chris, Chris will help to generate pdfs test reports for IEC audit and help to consolidate the test reports, currently he does not have any specific ideas for isar-cip-core meta-data testing
- **Testing for metadata (recipes)**
    - CB asked how they are tested
    - Static checks required?
    - [04/25] Jan: isar-cip-core a integration layer, need to think how to test the layer and changes in packages
    - [05/09] No update

cip-core-sec

- (No update)
- AI(Toshiba): Add improvements to solve some issues and make the project official (move to cip-project)
- AI(Toshiba): Update the ISAR gitlab-ci integration branch

Software Updates WG

- Related updates in isar-cip-core
    - swupdate: Enable SWUpdate for RZG2M
- **Support data encryption (secure storage)**
    - Targets
        - QEMU (ARM): WIP
        - QEMU x86 : WIP*
            - TPM emulation configuration required
        - Physical boards
    - [04/25] Jan: For both x86, arm64 data encryption is enabled also using TPM emulation
        - Need to plan testing of data encryption and SWUdate and others for complete image testing
    - [05/23] Data encryption with SWUpdate needs to be verified on QEMU

Q&A or comments

- **(Discuss in June...)**
- Do we have commitments to maintain any specific versions or all versions of isar-cip-core meta-data for SLTS period?
- What would be the process to address issues found on a specific version of meta-data e.g. if some issue is found on release V1.0, the fix will result in V1.0.1 release or the fix will be provided in the latest release of meta-data?
- Do we have plans to maintain branches for specific releases e.g. metadata version V2.x is used to generate Security images for BV testing and there might be some issue fixes..and finally meta-data version V2.Y is certified, we may have to separately maintain this in a branch?
- EOSS: Can we provide a demo of SWUpdate + secure boot using a physical board?
    - Jan: Provide slides / papers in booth about the latest features (e.g. secure boot, secure storage)
    - Another idea: show demos using physical board (x86, ARM64)
        - No physical boards with X86 TPM 2 ?
- Plan for CIP Core WG meeting in Prague
    - AI(Kazu): Collect information (discussion topics, persons,...)

Items that need approval by TSC voting members

- None