CIP Core regular meeting

- **Date: November 5th (Tuesday), 2024**
- 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
Andes	Tim Ouyang
Cybertrust	**Hiraku Toyooka** Arisu Tachibana
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)** **Koshiro Onuki** **Dinesh Kumar** **Sai Ashrith** **Shivanand Kunijadar** **Adithya BalaKumar**

Discussion

Action items updates

- AI(Kazu): Update WG wiki pages
- CIP Core package management for Debian LTS / Extended LTS
    - ~~AI(Kazu): Confirm ELTS funding costs for Debian 8 and 10~~
        - **(DONE): The estimated costs were shared with TSC/GB**
    - AI(Kazu): Update package proposal process & improve scripts
        - (WIP) Management script improvement
            - Refactoring for automation
            - Reviewing the MR
    - AI(Kazu): Package proposals
        - Waiting for the cip-pkglist script update above
    - **AI(Kazu): Create a proposal to decide which Debian versions will be supported**
        - From the F2F TSC meeting on Oct. 30th
- CIP Core testing
    - **AI(All): Enable OpenBlocks IoT in isar-cip-core & CI**
        - ~~Plat'Home will try to install & boot the generic x86 image~~
        - Toshiba confirmed the CIP kernel (x86 generic config) & CIP Core (x86 generic image) work with the device (USB memory boot)
        - Kernel WG is enabling kernel test with LAVA environment (NFS boot)
        - CIP Core will enable the test for this device as well once the test patterns are decided
- Deby
    - **AI(Toshiba): Update deby recipes to support the latest meta-debian**
- IEC 62443-4
    -
- Software Updates

-

CIP Core WG chair

- CTJ suggested Motai-san will take the WG chair role over
- AI(Kazu & CTJ): Clarify details in email

CIP Core package management for Debian LTS / Extended LTS

- Status summary:

Releases	Status	Recipes	Package list	Debian ELTS
8 jessie	Supported with 4.4 SLTS	Available (deby)	Minimum set: Approved	Active (2020-07-01~) List submitted Updating for 2025-H1
9 stretch	Unsupported	-	-	-
10 buster	Supported with 4.19 SLTS	Available	Minimum set: Approved	Active (2024-07-01~) List submitted Updating for 2025-H1
11 bullseye	Under discussion (work with 5.10 SLTS)	Available	Not proposed yet	ELTS not started yet
12 bookworm (current stable)	Under discussion (work with 6.1 SLTS)	Available	Not proposed yet	ELTS not started yet
13 trixie	Under discussion	Experimental	Not proposed yet	ELTS not started yet

    - FYI: The meaning of “Supported”:
        - 1. Make recipes available for the release (keep testing)
        - 2. Apply security fixes for (selected) packages of the release
            - Achieved by Debian ELTS funding, self-maintenance is not considered
- AI(Kazu): Update package proposal process & improve scripts
- AI(Kazu): Package proposals
    - Update & register package list for Debian 8
    - Update Debian 10 package list (add missing ELTS base packages)
    - Package proposal for Debian 11 & 12
- CIP members who demand those versions:
    - Debian 11
        - Toshiba
        - Siemens?
            - Jan: May require
            - Benjamin: Using
        - CTJ: Not using
    - Debian 12
        - Security WG
        - Toshiba

        - Siemens
        - CTJ
    - AI(Kazu): Ask other members' opinions then make proposal
- Milestones
    - ~~2024-10 Finish package list update for Debian 8, 10 (both ELTS)~~
    - 2024-11
        - Finish refactoring of cip-pkglist
        - Make a proposal to support Debian 11 & 12 (TSC)
    - 2024-12 Decide support plans for newer Debian releases (11, 12) also from budget perspective

IEC-62443-4

- Meeting with BV held on 24th Oct to clarify SWG queries
    - Why is SVV-4 (Penetration testing) missing in the BV test plan?
        - BV agreed to conduct penetration testing, it's not included as BV thought penetration testing is not applicable to CIP
    - How will SVV-1 to SVV-3 be executed and does CIP need to prepare something
        - BV plans to execute tests manually and CIP needs to share test reports on M-COM device
    - How FR-1 to FR-7 tests will be executed whether BV has some test suite automation or manually?
        - All test cases execution to be done manually
    - Test plan document shared by BV
        - https://docs.google.com/spreadsheets/d/14Mo-nCi5EooZIZdV6EqAbumJqDNqjUey/edit?gid=500607932#gid=500607932
- CIP side preparation for IEC-62443-4-2 final assessment
    - Provide details related to device (M-COM)
        - SWG working to update HW interface description document where details of each supported port, protocol used and how it will be secured needs to be provided
        - [**11/05**] it's in progress at Siemens side
    - Need to work on release process of images e.g.
        - Creating release notes with minimal information like kernel version supported, Debian version, CVE details etc
        - We can also add details of test results on the generated image using release tag of isar-cip-core
        - SWG add more items from IEC compliance perspective
        - Where to put the information?
            - CIP wiki page, release email, etc.
            - Test CI job
        - What information is required?
            - Should be automated

- Discussion in CIP Core meeting
    - Jan suggested to propose changes required in the release keeping in mind it is maintainable and most the information gathering can be automated
    - In case some information gathering can't be automated, then SWG and CIP Core WG members should work for releases to create minimum required documentation
    - SWG to further discuss and propose required changes
- [**10/22**]
    - SWG discussing on following changes for release process
        - List Open/Known issues
        - Provide CVE details
        - Test reports for the release
        - Security Release checklist update
        - Further discussion in progress
    - Few queries from SWG
        - When release happens can we run CI on the master branch instead of the next branch?
            - In some projects, releases happen when a new release tag is registered
        - FYI: running CI against master was redundant in isar-cip-core, thus was removed to save CI minutes
        - What should be the release target e.g. X-86 generic?
            -
        - Shall we generate reference images or not? Anything is fine as generating and maintaining images may include more complexities if there are no requirement
            - Currently images are not kept (images will be updated soon once master updated)
            - Providing artifacts require license compliance efforts
- [**11/05**]
    - SWG discussing list of items to be included in the release process, feasibility to automate etc

- Security image testing on M-COM
    - Remaining items
        - Update device setup document (Benjamin's patch)
            - Need to update minor issue (e.g. format), still pending
            - https://lists.cip-project.org/g/cip-dev/message/16631?p=%2C%2C%2C20%2C0%2C0%2C0%3A%3Arecentpostdate%2Fsticky%2C%2CBenjamin%2C20%2C2%2C0%2C107109743

        - Enable watchdog and verify roll back
            - Two WDT devices: I2C connected, UEFI watchdog of EBG
        - [**11/05**] No update and it's not high priority so let's remove it and keep it for future
- Investigation to generate test results on M-COM device locally in progress
    - Manual execution of LTP tests on security target in progress.
        - Because MCOM has not been in LAVA
- Functional test results of CIP kernel and CIP Core on MCOM are required
    - LTP
    - Security tests (CIP Core image)
    - Debian package test results
- SWG checking the existing policy for house keeping for maintaining CIP gitlab repos and AWS accounts
- Autopkgtests activities update
    - Fail2ban
        - MR was merged but there are few issues which are under investigation
            - MR:https://salsa.debian.org/python-team/packages/fail2ban/-/merge_requests/11
        - Issues are listed in isar-cip-core issue #6
    - Tpm2-tss
        - Toshiba has shared patches to enable autopkgtests for tpm2-tss package. The patches are under review
        - Planning to create BTS and attach patches as there is no response from maintainer so far
    - Core-utils
        - Maintainers does not want to add autopkgtest as he found there more issues caused by CI environment and he suggested to generate test results locally
        - It looks like already someone shared autopkgtest (2019) but they are not merged due to same reason
            - https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=927758
    - SWG Stefan is in discussion with Alpha-omega project members to get support for packages having no tests
    - They are ready to support adding tests for packages having no tests within certain budget, SWG creating final list of packages

Reproducible builds

- Actions from RB team meeting
    - **Resolve diffoscope performance issues**
        - Created an issue in the diffoscope repository under debian salsa for further discussion with RB team regarding the issue.
        - Suspended

- Reproducibility issues in generating CIP Core image
    - (1) Empty ext4 partition (/var) is not reproducible
        - rootfs hook seems not be run if the partition is empty
        - A patch for OE-Core was applied to master
        - Backported patch to isar merged to next branch.
        - We just need to wait for isar-cip-core update
        - **[10/22]** The fix for the issue is now available in isar-cip-core with the commit: 722ab2d23bb06108d4f0a0b6a0b75765289bfa40
        - All 3 QEMU targets in the weekly RB check is now passing as all partitions in the QEMU target are reproducible. Hence this issue can be closed.
        - CI:https://gitlab.com/cip-project/cip-core/isar-cip-core/-/pipelines/1503775955
    - (2) rootfs ext4 formatted partition size sometime varies
        - Blocks occupied in disk change in each build
        - rootfs contents are identical
        - There is a difference in the way the rootfs size is calculated in OE-Core and Isar. OE-Core uses a custom function to calculate the rootfs directory size. More information is explained in the below thread in isar ML: https://groups.google.com/g/isar-users/c/Ll7t4G41Lfo
        - Directory indexes (htree = hash tree) do not match across builds. Directories that occupy more than 1 filesystem block (normally 4096 bytes), are indexed using a hash tree to efficiently look up files.
        - **[11/05]** The directory indexes in the initial rootfs created by isar-bootstrap have identical structure, but after creating a copy the rootfs tree for the target rootfs, the index structure changes and are not consistent across builds.
            - What kind of copy method is used?
                - cp -Trpfx --reflink=auto
            - This command is isar specific, but the action itself is not isar specific. Let's collect information about how to make the action reproducible (file leve? FS level?)
        - Need to investigate further
    - (3) ext4 images created with IMAGE_CMD of isar are also not reproducible
        - Need investigation
- (WIP) Updating CI to check reproducibility of disk (wic) images
    - (Suspended) Will take this up once the existing RB issues are fixed.

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/
- Major updates (next) from the last WG meeting
    - efibootguard-boot.py: Add option to build without initrd
    - kas: Update to release 4.5
    - efibootguard: Update to 0.18 (Extend WDT supports)
- Recent releases
    - v1.5 (Oct. 22th)
- (WIP) EROFS support
    - Features comparing to squashfs (currently used for CIP Core)
        - Better read performance with/without compression
        - Potential of smaller delta between two images due to block level compression support
            - Worth to evaluate the actual delta size
        - Options to set variables that needs to be fixed for reproducible builds
            - Timestamp of all files, FS UUID
        - (Minor) ACL support, etc.
        - Comparison (erofs.docs.kernel.org)

deby

- (No update)
- AI(Toshiba): Update deby recipes to support the latest meta-debian

CIP Core Testing

- AI(All): Enable OpenBlocks IoT in isar-cip-core & CI
- Testing with physical boards
    - Only QEMU targets are used for testing now
        - Pipeline example
    - **Issue 1: Board list for CIP Core testing**
        - NOTE: Need to implement method to install disk image then test
        - Siemens MCOM (Security WG)
        - MPSoC ZCU102 (CTJ)
    - **Issue 2: Methods to install disk image automatically before tests**
        - LAVA supports two steps testing: Installation => boot for testing
        - Needs firmware/bootloader which is not overwritten by the installation step (EFI, U-Boot)
    - **Issue 3: Optimization of test patterns**
        - Max: # of boards * Image features * test cases
        - **What are the cases that can be dropped from CI?**
- ~~**[11/05] CIP LAVA Lab maintenance update**~~

    - Chris confirmed LAVA Lab maintenance done by administrators by the end of last week.
    - After the maintenance no LAVA infrastructure related errors are observed.
        - We can close this issue

Debian 13 trixie support

- trixie will be released around 2025 summer
- Will CIP Core support Debian 13?
    - (Members opinions...)
- EFI Boot Guard issue due to gnu-efi update
    - Issue update
    - Fixed in the upstream
- riscv64 support
    - riscv64 will be the official architecture from Debian 13
    - Kernel & Core image (Debian sid based) are working on QEMU riscv64
    - Should riscv64 be one of the supported architectures?
        - (Requirements from members...?)
    - Which physical board should be the reference H/W for testing?
        - Renesas RZ/Five
            - ILM and DLM blocks of the AX45MP (RISC-V core) exist within 0x30000-4ffff which is not handled by MMU
            - Problem: Some libraries (i.e. .debs) that assume TEXT_START_ADDR=0x10000 need to be recompiled by changing the address due to the address conflict
            - No solution at the moment (rebuild base libs by CIP requires too much effort and inefficient)
        - Others
    - Will riscv64 be supported by LTS/ELTS (Freexian)?
        - It's too early to check now. Let's check after trixie becomes stable at earliest.
- Other topics?

CVE Checker

- ~~**Checking cause of CI job stuck issues with the small runner**~~
    - **[10/22]** Chris sent a patch to use large runners to run cve-checks job. It is merged into the master branch.
    - **[11/05]** We can conclude CVE checker job requires non large runner

License compliance process in Debian

- [9/10] Comments from Jan

    - License compliance process in Debian side (“planned” activities)
    - What Debian can do for downstream users?
    - In DebConf, there were discussions about collect information
    - Raising ideas from us to Debian
    - Related talk in DebConf: A BoF session (not recorded!)
        - Abstract: To be checked
    - We can also discuss from the IEC perspective
- FYI: CTJ created scripts to create SBOM information of isar-cip-core

Software Updates WG

Support Reference H/W

- (No plan to support new boards at the moment)

wfx

- **(WIP) Enable wfx service as wfx.cipatform.org**
    - LF support thread to request the cloud settings
    - Service proposal (TSC voting) (due date: Oct. 29th)
        - Mostly approved?
- Adjust isar-cip-core recipes to enable wfx (client)
    - Previous discussions
    - **[11/05]** (No update)
- Enable regular CI to test the device update with wfx (DAU)
    - (Not started yet)
- PoC for multiple device update based on demands in practical cases
    - (Not started yet)
- Debian packaging?
    - Currently building with go build
    - https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1057366 / ITPed
    - (No update)

Secure update framework (TUF)

- Milestones
    - 2024-09 : (Done) Finish implementation & Demo@osse2024
    - **2024-10 : (Done) Demo@ossj2024**
        - **https://youtu.be/Hrk5WpA7jBA?si=_e6Bhv_ecV1rMifL**
        - **Some fixes for the demo couldn’t be completed in time, so we will postpone them for now.**
- The integration of SWUpdate & TUF (w/ RS-TUF)
    - **[11/05]** (No update)
    - (DONE) New TUF-client:

            - TUF-client is compiled into .so to be used in Lua (swupdate_suricatta.lua)
        - Next topic
- Archive
    - Prototyping CIP Core + SWUpdate + TUF example with RS-TUF
        - https://gitlab.com/cip-playground/cip-tuf-demo/-/tree/v0.2.0
        - Device can check available updates, download and install using TUF
            - Server: RS-TUF
            - Client: go based implementation
        - Support device status management with wfx
            - It's not a DAU workflow, but a custom workflow we created
        - Automate flows to create swu images
        - Support for creating delta update (rdiff)
        - Implementation is also verified with the MCOM device
        - Simple GUI for demonstration

Delta update support

- Milestones
    - **2025-01: Summarize the results**
    - **2025-02: Support binary files (e.g. UKI) in recipe, if necessary**
- Continue to evaluate delta update functionality
    - Summarize the results regarding image delta reduction and performance
    - Support binary files such as kernel images
    - **[11/05]** Started investigation to support kernel image, no much updates at the moment.
- Minor topics
    - Zchunk with MCOM
        - Zchunk update with MCOM verified with Sid image from isar-cip-core master branch
            - Need to use sid version SWUpdate package instead of bookworm-backports due to some issues

Test automation with LAVA

- Milestones
    - 2024-12 : Verify the tests with MCOM
    - 2025-03 : Add / improve tests especially for security
- Verify the tests with MCOM
    - Waiting for the device is connected to LAVA (Siemens lab)
    - **[11/05]** Bjorn confirmed that M-COM x86 arrived at Siemens, Prague. Awaiting a tentative date when M-COM x86 shall be connected to LAVA Lab.

- Add / improve tests
    - e.g. Failure cases of secure boot
    - (No update)
    - **[11/05]** Identified following fail-case scenarios for secure boot testing:
        - Trying to boot with an unauthorized kernel image.
        - Trying to boot with an unauthorized root filesystem (verity-device corrupted).
    - **[11/05]** Zchunk delta update testing.
        - However it can be tested only for sid/trixie version.

Open Source Summit Japan 2024 Demo preparation (Completed)

- Few enhancements under discussion for the demo at OSS-J
    - Automate starting SWUpdate to poll for updates as soon as image boot [In-progress]
    - Also automatically confirm status back to WFX [In-progress]
        - **[11/05]** The swupdate service sometimes fails due to problems with refreshing tuf-metadata. The issue is inconsistent and usually is not seen when the swupdate service is manually restarted.
        - **[11/05]** Needs more investigation.

Q&A or comments

- None

Items that need approval by TSC voting members

- None