CIP Core regular meeting

- **Date: October 8th (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 (Absent on 2024-08-27)
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 page
  - ~~[9/10] WIP: Adding RB introduction page~~ (DONE)
    - https://wiki.linuxfoundation.org/civilinfrastructureplatform/reproducible-builds
    - https://reproducible-builds.org/who/projects/
- Debian Extended LTS
  - AI(Kazu): Update package proposal process & improve scripts
    - Add “confirm maintenance plan of ELTS”
    - [9/10] (WIP) Management script improvement
      - Refactoring for automation
        - **[10/08]** Toshiba has created a MR to refactor the pkglist scripts. Review in-progress.
        - MR:https://gitlab.com/cip-project/cip-core/cip-pkglist/-/merge_requests/17
        - **Query**: Currently only buster pkglist is included in the repository. Should the scripts also support proposing packages for suites that don’t have a pkglist in the repository (Ex: bookworm).
          - See the summary table in Extended LTS
      - Support ELTS infrastructure (e.g. security tracker)
  - AI(Kazu): Package proposals
    - [9/10] On-going
    - Update & register package list for Debian 8
    - Update Debian 10 package list (add missing ELTS base packages)
    - Package proposal for Debian 11 & 12
- CIP Core testing
  - AI(All): Enable OpenBlocks IoT in isar-cip-core & CI

        - Plat'Home will try to install & boot the generic x86 image
            - [10/8] No update
- IEC 62443-4
    -
- Software Updates
    -

Debian LTS / Extended LTS

- Status summary:

Releases	Status	Recipes	Package list	Debian ELTS
8 jessie	Supported	Available (deby)	Minimum set: Approved **(but need to be updated)**	Package list shared
9 stretch	Unsupported	-	-	-
10 buster	Supported	Available	Minimum set: Approved **(but need to be updated)** **openssl: Already included**	ELTS will start on 2024-07-01 Draft package list shared
11 bullseye	Under discussion	Available	Not proposed yet	ELTS not started yet
12 bookworm	Under discussion	Available	Not proposed yet	ELTS not started yet

- 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

IEC-62443-4

- Meeting with BV for initiating IEC-62443-4-2 assessment held on 1st oct
    - CIP SWG explained again about CIP project and activities as there are new members involved now
    - SWG highlighted roadmap shared by BV will need some extension as CIP side all task may take more time to complete
    - BV clarified HW features supported by M-COM will be assessed and mentioned in the detailed report
    - Any features not supported by M-COM e.g. wireless network support will be marked as N.A.
- 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
    - 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
    - Once HW interface description document is ready, SWG will update threat modeling document to include details of device security
    - Finalize version of isar-cip-core metadata and CIP kernel for creating security image for evaluation
        - This can be the next isar-cip-core release??
        - v1.5 will be released around the middle of Oct.
    - Run IEC layer tests on final image in M-COM and confirm results
        - In last isar-cip-core (V1.4) all tests passed
- CIP IEC documents are available in readthedocs format, it's generated from master branch
    - https://cip-documents.readthedocs.io/en/latest/
    - All the pdfs are automatically generated once some change is merged
        - https://gitlab.com/cip-project/cip-documents/-/jobs/7964435199/artifacts/browse/rstPDF/
- 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
- Toshiba shall send an MR to fail2ban to add necessary changes to run existing tests in the repository as part of autopkgtest.
    - This helps to understand the roadmap to enable autopkgtest for remaining packages which are not tested as part of Debian CI in the security image.
    - **[10/08]** Toshiba shared MR to fail2ban for adding autopkgtest support. MR merged in fail2ban salsa repository.
        - MR:https://salsa.debian.org/python-team/packages/fail2ban/-/merge_requests/11
        - There are few failed test cases while running autopkgtest, Toshiba is currently investigating the cause for the failures.
- Implementation & verification of required features for IEC requirements
    - NDR 1.6 & NDR-1.6 RE(1)
        - Wireless access management
        - In case if there are use cases to support wireless access, we need to add required packages and services
        - MCOM does not have on-board wireless devices.
        - [**10/08**] As per BV features supported by M-COM will be reviewed and approved hence support for wireless network access can not be confirmed
    - EDR-3.10 & EDR-3.10 RE(1)
        - Support for software updates & upgrade
        - Most of the support is verified on M-COM
        - Issue: Update image encryption is not “enabled” by default
    - EDR-3.14 & EDR-3.14 RE-1
        - Support for integrity of the boot process
        - May be no action required for X-86 at least as on M-COM device it’s supported
    - CR 1.4
        - Identifier management where component can integrate with other system for identification
    - CR 7.3
        - Control system backup
        - Already concluded as part of survey needs to discuss further with BV
    - Survey results for wireless network support in CIP
        - Two CIP members confirmed they have devices with wireless network support (Wi-Fi and Bluetooth)
            - Renesas: RZ/G2M HiHope EVK

            - Moxa: Moxa industrial computer
            - Toshiba: None
        - For meeting IEC-62443-4-2 NDR 1.6 & NDR-1.6 RE(1) , CIP members should decide whether to include any additional drivers/packages to meet this requirement
    - [**09/10**] This topic is still not discussed with BV
- Package test evidence
    - **No task pending for IEC now**
    - Summary of each package status
    - Securit WG is asking package / upstream maintainers requirements / plans about adding tests for the future
    - **[10/08]** Security WG plans to contact maintainers of packages that have tests but aren't run as autopkgtests to identify if there is any roadmap to add autopkgtests in the near future. This helps Security WG identify which packages to contribute to by adding autopkgtests. Totally there are **68** packages that belong to this category.
    - **[10/08]** Security WG also contacted maintainers of packages that do not have tests defined in either debian or upstream. Totally there are **19** packages that belong to this category. Majority of the maintainers confirmed that there are no tests defined currently but contributions from members are welcome.

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.
        - [09/10] No update on this issue
        - Kazu: It's one of the ways to close the issue if the problem does not happen with the latest CIP Core image for a while. (then reopen anytime if it's reproduced)
    - Share CIP's results in RB home page
        - WIP (Kazu)
- 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
    - (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.
        - Need to investigate further
        - **[10/08]** No update on this issue.
    - (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
    -
- Recent releases
    - v1.4 (June 25th)
    - v1.5 will be released around the middle of Oct.

deby

- (No update)

CIP Core Testing

- AI(All): Enable OpenBlocks IoT in isar-cip-core & CI
- [8/27] isar-cip-core CI
    - Some tests are failing (IEC, swupdate)
    - Causes are not clear (tests themselves or infrastructure issues)
    - Regarding the both IEC & swupdate tests, issues we observed previously should be fixed already
    - One issue is that in some tests a device reset again and again, then timeout happens
        - Only happening with certain LAVA labs (not all)

- [09/10] Made a list of all failure jobs in LAVA due to inconsistent issues leading to timeout errros such as
    - QEMU reset during boot
    - Low download of artifacts
    - Slow encryption of /home and /var during boot

  Occur only in lab-cip-siemens-muc.

    - It is also not the case that every job running in lab-cip-siemens-muc fails due to the above-mentioned issues. The behavior is unpredictable.
    - Need to debug the cause of these issues in the lab-cip-siemens-muc.
    - To avoid these failures until then, the **swtpm-jobs** tag can be temporarily removed from the qemu-cip-siemens-muc so that the test jobs triggered from isar-cip-core CI will not be assigned to the mentioned QEMU device.
    - Quirin suggested the same and Chris removed **swtpm-jobs** tag from qemu-cip-siemens-muc.
    - A connectivity issue in the lab is observed, which will be fix in the future (but and others)

CVE Checker

- As Debian buster moved to ELTS, Toshiba is working to change the source URL to freexian in case the suite is buster
    - Related issue: https://gitlab.com/cip-project/cip-core/debian-cve-checker/-/issues/1
- **[08/09]** MR to handle Debian buster for cve-reports merged in debian-cve-checker.
    - Changes are verified in isar-cip-core CI. Patches to update image reference in isar-cip-core shall be sent for review.
- **[08/27]** Patches (A, B & C) to update debian-cve-checker reference in isar-cip-core CI merged.
- **[09/10]** cve-checks job gets stuck in the middle when using “small” runners leading to “pods runner-zwslwy9eu-project-10191315-concurrent-0-2fdr4qlb not found” error.
    - Michael Adler suggested trying again considering it might be a temporary issue. He mentioned that there are no issues with the runners.
    - Even after several retries after that, the issue still exists.
    - The job runs successfully with “large” runners.
    - Example of the stalling jobs: xxx
- **[10/08]** Chris sent a patch to change small runners to large to run cve-checks job. It has been merged into isar-cip-core.
    - Chris tried to debug the issue with cve-checks job getting stuck in between. He mentioned small runners use t3.small EC2 instances which have 2 vCPUs.

    - Based on his analysis, he said multiple jobs run parallelly on these small runners and it is not enough to run cve-checks.
    - While accepting the patch, Jan asked whether we are trying to understand what might have been wrong with the small runners. This point has to be discussed with Chris.

Software Updates WG

Support Reference H/W

- Secure boot, secure storage support for CIP reference HW

Reference H/W	SWUpdate	Secure boot	Secure storage
QEMU	Supported	Supported	Supported
BBB	Supported	-	-
Renesas RZ/G2M	Supported	-	-
Siemens MCOM	Supported	Supported	Supported
Siemens IPC227E	Supported	-	-
Others	Not supported	Not supported	Not supported

-
- Siemens M-COM
    - Benjamin : Planning to hand carry the device to OSS-J

wfx

- [9/10] Provide wfx.cipatform.org
    - Asking LF to update cloud settings
- Plans
    - (1) Permanently run a wfx service (instance) in a CIP site (something like https://wfx.ciplatform.org/)
        - Use the upstream docker image
        - If CIP detects issues / missing functions, try to resolve them in upstream if possible
        - Resolve things that downstream has to do by the existing mechanism to integrate user-defined middleware
            - Ref: https://github.com/siemens/wfx/issues/43
    - (2) Run device update tests with wfx (DAU) for CIP Core image installed devices
        - Update isar-cip-core recipes to configure wfx client (i.e. use server_wfx.lua, configure swupdate.cfg)

        - Add test cases for LAVA to do device update through wfx server (1) into https://gitlab.com/cip-playground/cip-core-ci
    - (3)(Lower priority) Create an UI tool for wfx
        - The first target is a ready-to-use UI for future CIP demos
        - Stretch goal: Consider possibilities of providing an (flexible) UI tool that can be adapted to new/existing services in fields where no UI so far
    - (4) Create an enhanced demo for OSS-EU 2024 using outputs of (1)(2)(3)
- About (2): Update isar-cip-core recipes to enable wfx
    - Initiated discussion with CIP community in cip-dev ML to better understand on how to go about the integration of WFX backend with CIP images.
        - Discussion link: https://lists.cip-project.org/g/cip-dev/topic/regarding_support_for_wfx/106775534
        - Summary: 2 parameters are mandatory in the swupdate.cfg file
            - WFX server URL
            - Client-id
        - Setting the WFX server URL could be achieved by a kconfig variable which the user has to provide before the build.
        - Normally client-id is usually received upon device registration from an on-boarding backend. Do CIP images now also have to provide a device on-boarding mechanism? Currently under discussion in ML
            - Start by PoC
        - Based on suggestions from Christian, WFX integration could be achieved by the following:
            - Create an on-boarding workflow and a corresponding client to receive the configuration data (in this case, client Id)
            - Clients can get the on-boarding WFX job id upon first onboarding request with the necessary device information (like device serial number) and use wfx plugins to process the request appropriately.
            - By this the devices get their identity (client-id) at run time during on-boarding.
        - **[10/08]** No update regarding this task.
- Other topics
    - Debian packaging? (Currently building with go build)
        - https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1057366 / ITPed

Secure update framework (TUF)

- Milestones

        - 2024-09 : (Done) Finish implementation & Demo@osse2024
        - 2024-10 : Demo@ossj2024
- Proceed with improving the system using RS-TUF as the reference implementation of TUF
- 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
    - 2024-5 : (Done) Finish isar-cip-core integration
    - 2024-8 : (Done) Verify typical use cases including backend
    - 2024-9 : (Done) Demo
- Continue to evaluate delta update functionality
    - Summarize the results regarding image delta reduction and performance
    - Support binary files such as kernel images
- 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
    - 2024-6 : Finish cip-core-ci implementation for SWUpdate testing and enable CI (Done with QEMU)
    - 2024-X : Verify the tests with physical boards (at least MCOM)
        - Automation is not mandatory for IEC
        - Let's check when the board will be connected to LAVA
- Suspended

- **[08/27]** No updates because the M-COM device has not been added to CIP LAVA Lab yet.
- [**10/08**] Moxa is working to ship M-COM device to Prague to use it for CIP LAVA testing

Other topics (not started yet)

- Hardening secure boot & secure update
    - e.g. Artifact signing

Open Source Summit Europe 2024 Demo preparation (Completed)

- Main topic: TUF integration
    - RS-TUF based (Step2)
    - Include GUI for demo
    - Run on MCOM
    - Delta update (rdiff) supported
    - Update status is managed by wfx
    - ~~Negative testing focusing on advantages of TUF?~~ => Skip this time...
- Slide
    - Explain whole Software Updates WG activities
    - TUF, wfx, delta update, test environment
- Leaflet (Hand-out)
    - P.1 CIP overview, WG introductions
    - P.2 Description of TUF integration + short introductions of other three topics
- Devices
    - Siemens MCOM & power adaptor (Bjoern)
    - A laptop as host PC (Dinesh)
        - No internet connection is required while demo
    - Monitor
        - Provided by LF
    - Devices to re-install CIP Core image to MCOM
        - USB memory (Dinesh)
    - Power plug
        - Provided by LF
        - We can use three sockets (laptop, MCOM, monitor)
- [09/10] Demo slides and leaflet shared for CIP member's review. See the cip-members ML.
- [09/10] Instructions regarding demo setup with MCOM shared with Siemens members.

Open Source Summit Japan 2024 Demo preparation

- Few enhancements under discussion for the demo at OSS-J **(Tentative)**
    - Support MQTT based device status monitoring.
    - Automate starting SWUpdate to poll for updates as soon as image boot.
    - Also automatically confirm status back to WFX.
- Updates to leaflet and slides based on updated demo topic.
- Initiate discussion for booth and equipment requirements

Q&A or comments

- **[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**
- **[9/10] Dinesh: MCOM device in MOXA**
    - **If no plan to use, we would like to suggest other ways e.g. putting this to LAVA, using the device for OSS-J 2024 demo, etc.**

Items that need approval by TSC voting members

- None