

CIP Core regular meeting

- **Date: May 7th (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
Bosch	Philipp Ahmann Sietze van Buuren
Cybertrust	Hiraku Toyooka Arisu Tachibana
Hitachi	
Linutronix	
Moxa	Jimmy Chen
Plat'Home	Masato Minda
Renesas	Chris Paterson Kento Yoshida Kazuhiro Fujita Hung Tran

- Benjamin has joined the discussion, if anyone has any comments or what is the current status of this work, we would like to know
- [04/23]
 - Recently Plat'Home OpenBlocks IoT VX2. configs are added to generic configs list
 - Discussion on-going
 - <https://lists.cip-project.org/g/cip-dev/message/15547>
- [05/07]
 - Recently Quirine is working to integrate x86 kernel configs and shared integrated changes
 - <https://lists.cip-project.org/g/cip-dev/message/15823?p=%2C%2C%2C20%2C0%2C0%2C0%3A%3Arecentpostdate%2Fsticky%2C%2Ckernel+config%2C20%2C2%2C0%2C105891053>
 - Next step: Create a MR for cip-kernel-config
 - First, resolve minor issues
 - We have to test the config with x86 targets
- debian-cve-checker
 - Al(Toshiba): Move it to cip-core sub group
 - [5/7] No update
- IEC 62443-4
 -
- Software Updates
 - ~~Al(Kazu): Consider creating a proposal to include wfx in the CIP project~~
 - Terminated. Currently no plan to include wfx itself in the CIP project. We will reconsider when it will be a necessary topic.

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 (confirm maintenance plan of ELTS)
- AI(Kazu): Update & register package list for Debian 8
- AI(Kazu): Update Debian 10 package list (add missing ELTS base packages)
- AI(Kazu): Package proposal for Debian 11 (again)
- AI(Kazu): Check the infrastructure in ELTS like BTS, security tracker, etc. and how CIP can communicate with them using such system in the future
- [5/7] No update

IEC-62443-4

- SWG working on revising CIP IEC-62443 assessment schedule, it has some dependencies on M-COM device recipe integration to start IEC-62443-4-2 assessment, would like to know any comments
 - https://docs.google.com/spreadsheets/d/1A8VBLCg01tW2Xz_OBGV8ChdPz21r5y5N/edit#gid=699836056
 - Based on current situation, SWG will consider to revise schedule and start 4-2 assessment from B/Jun
- What's the plan from Siemens to integrate M-COM recipes to isar-cip-core?
 - According to Benjamin M-COM device can boot with Siemens SIMATIC IPC227E device image
 - Now we need to discuss whether new recipes for M-COM device should be created or re-use SIMATIC device recipes
 - isar-cip-core: would like to have a generic H/W configuration for x86 boards. The current question we have is how to implement generic kernel (config) for x86. Need to reboot the previous discussion.
 - AI(Dinesh): Reboot the previous discussion.
 - [03/26] Benjamin from SWG has joined the discussion related to X86 generic kernel configs, SWG would like to understand what's the current status, can someone summarize it or confirm when it can be completed?
 - [04/23] Sorry I could not attend kernel WG meeting to discuss if there is any detail plan available for implementing general kernel configs
 - **[05/07]** Based on patches shared by Benjamin for adding M-COM device as target, we have created M-COM image. However booting is yet to confirm due to power adaptor unavailability (Benjamin patches)
 - <https://lists.cip-project.org/g/cip-dev/message/15808?p=%2C%2C%2C20%2C0%2C0%2C0%3A%3Arecentpostdate%2Fsticky%2C%2Cbenjamin%2C20%2C2%2C0%2C105862262>
 - Once Quirine changes for making X86 kernel configs are merged, we can create M-COM images based on CIP kernel 6.10

- CIP Core essential package list
 - Investigation for packages which have Debian CI results whether they have functional tests
 - <https://docs.google.com/spreadsheets/d/1rOHJUhUOa05Kkn4typfczSZTtKWc1YoL/edit#gid=32781124>
 - Contacting with package maintainers to understand plan for adding tests in progress
 - During next BV meeting, SWG plans to discuss overall investigation so far and understand if there are any concerns from BV
 - Adding tests for all packages installed on security image may take very long time
 - What are the options available to meet the IEC requirement?
 - **[05/07]** SWG completed investigation of all packages having Debian CI results, which now includes what type of tests are included in Debian CI for 140 packages
 - SWG initiated discussion with BV and according to BV CIP can define process how to handle packages having no tests so SWG having discussion about how to conclude it
- M-COM device shipment updates
 - Siemens shipped M-COM devices to BV, Toshiba India and Moxa
 - BV confirmed two devices received
 - Moxa received one device
 - Toshiba India received one M-COM device, trying to purchase on power adaptor locally
- **LAVA IEC layer test automation**
 - **[05/07]** Some IEC layer test cases depend on syslogs to decide whether respective 4-2 requirements are satisfied. Syslogs are not present in the current CIP security image after this [patch](#) by Felix.
 - **[05/07]** Discussion with Felix to fix this issue in progress.

Reproducible builds

- Reproducibility issues in generating CIP Core image
 - No open issue
 - All required patches are merged in upstream projects (OE-Core, isar). Waiting for isar-cip-core pulls the fixes.
 - Close [open isar-cip-core issues](#) once required fixes are applied
- (WIP) Updating CI to check reproducibility of disk (wic) images
 - Waiting for isar-cip-core pulls the fixes
- (WIP) Fetch Debian packages from snapshot instead of live mirror
 - **[05/07]** ISAR currently supports building against snapshots when RB is requested. CIP can utilize this support for RB.
 - [Related commit](#) (isar master)

- Still not in isar-cip-core
- No additional setting to do in isar-cip-core than setting the flag (ISAR_USE_APT_SNAPSHOT = 1)
- Differences between s.d.o and snapshot-cloudflare.debian.org ?

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)
 -
- Recent releases
 - [v1.3](#) (Feb. 8th)
 - v1.4 -rc1 : delta update, rootfs encryption, others?

deby

- (No update)

CIP Core Testing

- AI(All): Enable OpenBlocks IoT in isar-cip-core & CI
- AI(All): Enable Siemens MCOM in isar-cip-core & CI

debian-cve-checker (old project: cip-core-sec)

- <https://gitlab.com/cip-playground/debian-cve-checker>
- [Sample output \(Excel\)](#)
- AI(Toshiba): Move it to cip-core sub group

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	WIP	WIP	WIP
Siemens IPC227E	Supported	-	-
Others	Not supported	Not supported	Not supported

-
- Renesas RZ/G2M
 - Enable secure boot
 - [5/7] We would like to cancel this item. Previously the intention is to add RZ/G2M to current secureboot support in CIP-Core, only the opensource part (similar to swupdate). But at the end it still requires Secure Storage (which is platform dependent), so it is not possible.
 - Kazu: OK, let's cancel
- Siemens M-COM
 - [5/7] Toshiba: Waiting for MCOM is available (power cable)
 - Benjamin : Planning to hand carry the device to OSS-EU

wfx

- Plans
 - Create a wrapper project for demonstration
 - Like [cip-tuf-demo](#), but no dependency on TUF stuffs?
 - Run tests regularly? (e.g. Run wfx server on AWS)
 - Debian packaging?
 - <https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1057366> / ITPed
 - Currently building with go build

Secure update framework (TUF)

- [5/7] Toshiba: Submitted OSS-EU 2024 CFP
- (WIP) Prototyping CIP Core + SWUpdate + TUF example with RS-TUF
 - Step 1: Minimum device update using RS-TUF
 - Client can upload update images
 - Device can check available updates, download and install
 - No device status management (state, version)
 - Step 2: Basic device update for typical use cases
 - Support device status management (probably with wfx)
 - Automate flows except image upload by clients
 - Improve tuf-client for SWUpdate
 - Milestones
 - 2024-4 : Finish step 1 implementation
 - 2024-9 : Finish step 2 implementation & demo

- Status
 - [5/7] No update? : Finished Step 1 PoC, updating cip-tuf-demo
- Others
 - Verification with delta update
 - Uptane evaluation

Delta update support

- Milestones
 - 2024-5 : Finish isar-cip-core integration
 - 2024-8: Verify typical use cases including backend
 - 2024-9 : Demo?
- (WIP) Prototyping delta update methods for CIP Core image
 - [05/07] Patches (v5) sent to integrate Delta Update in isar-cip-core in the CIP mailing list. Link: <https://lists.cip-project.org/g/cip-dev/message/15841>
 - Feedback received from the community for v4 was to have a default option for delta update type for easier usability, defaults can be overwritten via config (delta-update.yml) file.
 - **v6 sent to the ML then applied to the next branch, thank you!**

Test automation with LAVA

- Milestones
 - 2024-6 : Finish cip-core-ci implementation for SWUpdate testing and enable CI
- Status:
- **[03/26]** Toshiba made changes based on review comments provided by Chris on this [MR](#) . Waiting for Chris's approval.
- **[03/26]** Instead of directly storing all the job definitions in the repository, Toshiba created an MR using which the definitions are created from templates. Currently this [MR](#) is under Chris's review.
- **[05/07]** MRs [1](#) and [2](#) are merged after Chris's approval
- **[05/07]** Jan provided his opinion to use [cip-core-ci](#) in isar-cip-core to test when changing code.
- **[05/07]** Do we need to run test cases for three functionalities (Secure boot, SWupdate and IEC layer) at once whenever a pipeline runs in isar-cip-core ?
- **[05/07]** Approximate time to finish all the tests in LAVA is around 70 minutes. So the test job in the isar-cip-core pipeline should be running for such a long time to keep fetching the results of all the LAVA jobs.
 - Q1. Can we run multiple tests in parallel? => Yes
 - Q2. Can we reduce test executions? => Toshiba will send a draft patch for discussion
 - e.g. when merged into a specific branch
 - e.g. Test only when related functions are changed

- **[05/07]** Considering the cost issue, can we consider having 3 manual test jobs in each pipeline, one test target for each feature ? Based on the requirement, the person running the pipeline can trigger the required job for testing.
- **[05/07]** In this way we can avoid running these jobs for changes which are completely unrelated to what we are testing.
- **[05/07]** Planning: Create test results of SWUpdate/secure boot tests with SQUAD
 - Created a local SQUAD setup with LAVA.
 - Currently facing issues while sending SQUAD watch job requests. Discussion with CIP testing WG members in progress

Other topics (not started yet)

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

Q&A or comments

- None

Items that need approval by TSC voting members

- None