CIVIL INFRASTRUCTURE PLATFORM

CIP Core regular meeting

- **Date: April 23rd (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** 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)** **Koshiro Onuki** **Dinesh Kumar** **Sai Ashrith** Shivanand Kunijadar **Adithya BalaKumar**

Discussion

Action items updates

- AI(Kazu): Submit OSS-EU 2024 CFP about Reproducible Builds
  - Created a draft (see “RB” section below)
- AI(Kazu): Update WG wiki page
  - [4/23] No update
- Debian Extended LTS
  - [4/23] No update
  - 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
- CIP Core testing
  - AI: Enable OpenBlocks IoT in isar-cip-core & CI
    - (WIP) Patches are under review: 1(Merged), 2(Consider x86-generic)
    - Now, x86-generic kernel config is being considered in kernel WG
  - AI(Dinesh): Share the information and plan of x86 generic config for CIP kernel & CIP Core with the Siemens developer and reboot the remaining discussion (i.e. generic x86 kernel config)
    - Related thread: https://lists.cip-project.org/g/cip-dev/topic/100907933#12832
    - Also, you may be able to find some related notes in the last extended TSC meeting on Dec (before OSSJ)

        - 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
- IEC 62443-4
    -
- Software Updates
    - AI(Kazu): Consider creating a proposal to include wfx in the CIP project

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
- [4/23] 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
    - Can we assume M-COM device image with X86 based generic kernel config will be ready by M/May or E/May?
    - Siemens members will patches to integrate (the initial) recipes (SWUpdate, secure boot) for MCOM
        - Not much to do from features perspective
    - Possible variations: e.g. RT
- Should we ask one more MCOM for (Toshiba) Japanese members?
    - Kazu: Not mandatory, but it's helpful for demo preparation
- 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
- 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?
- 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

        - Shipment of one M-COM device available in Siemens India under consideration

- ~~**LAVA IEC layer test automation**~~
    - CIP security image is booting fine in LAVA after adding user defined commands (**Initializing swtpm socket**) to run in the LAVA dispatcher.
    - [03/26] Toshiba prepared MR mentioned below which has changes to remove dependency to install sshpass package in the security target before running IEC Layer tests. It is merged in master.
        - https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/merge_requests/15
        - This MR is merged, no updates pending
    - [04/23] Dinesh: Please remove the above information as nothing is pending now => Nothing, removed

Reproducible builds

CIP Reproducible build status

	Reproducible Build Status		
Target	**Raw contents**	**Filesystem Images**	**Disk Images**
QEMU AMD64	**Reproducible**	Reproducible*	Reproducible*
QEMU ARM64	**Reproducible**	Reproducible*	Reproducible*
QEMU ARMHF	**Reproducible**	Reproducible*	Reproducible*
BBB	**Reproducible**	Reproducible*	Reproducible*

* [03/12] Currently patches for ext4 and wic image reproducibility are accepted by the OpenEmbedded Core community. ISAR repository needs to be updated to bring these changes.

Raw contents:

- Artifacts built as raw files (vmlinuz, initrd, rootfs, linux.efi, swu file)
- Features enabled: Base + swupdate.
- CI pipeline: Pipeline · cip-project / cip-core / isar-cip-core · GitLab
- Contents:

File name	Status
vmlinuz	**Reproducible**
initrd.img	**Reproducible**
linux.efi	**Reproducible**
Rootfs (squashfs)	Reproducible*
swu	**Reproducible**

Filesystem images:

- Artifacts build with their Filesystems: EFI(vfat), boot(vfat), rootfs (squashfs), home(ext4), var(ext4)
- Features enabled: Base + swupdate + secure boot + security configurations
- CI pipeline: Pipeline · cip-project / cip-core / isar-cip-core · GitLab
- **File system images**:

Partitions	Status
EFI (vfat)	**Reproducible**
BOOT0 (vfat)	**Reproducible**
BOOT1(vfat)	**Reproducible**
Rootfs (squashfs)	Reproducible*
Home (ext4)	Reproducible*
VAR (ext4)	Reproducible*

- Issues:
  - #74 ext4 file system images are not reproducible **(Patches are accepted by OE-Core, isar needs to bring these changes)**
  - #75 The var partition image is not reproducible **(Patches are accepted by OE-Core, isar needs to bring these changes)**
  - #78 BBB ext4 images are not reproducible (**Fix applied in master branch of isar**)
  - #85 EFI and BOOT partitions are not reproducible (**Fix applied in master branch of isar-cip-core**)
  - #94 swu files are not reproducible from different days
    - [03/12] Patch to fix the issue sent to ISAR. Patch is merged to next branch in ISAR. Patch link: https://groups.google.com/g/isar-users/c/BBapJpQGinQ
  - [04/23] #103 .swu file not reproducible
    - Fix applied to master branch of isar-cip-core

Disk images: (Completed)

- Artifacts built as bootable disk images with partition table included.
- Features enabled: Base + signed swupdate + secure boot + security configurations.
- CI pipeline: **Waiting for upstream patches [04/23]**
  - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/tree/tsip/rb-wic-image-check
  - Changes are ready but verification with upstream patches pending
- Issues:
  - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/58 (Fixed in upstream with this patch)
  - #91 .wic images are not reproducible (**Completed**)
    - [02/13] Patches (v2) shared with OE-Core and isar-cip-core and merged in respective projects.
      - OE-Core: https://github.com/openembedded/openembedded-core/commit/150e079589e207fe174d2dceb40cd8f3d3972c5a
      - isar-cip-core: https://gitlab.com/cip-project/cip-core/isar-cip-core/-/commit/38703cb8e44f0dcdb3a1d7adccd765b861cf1273
- Others
  - Other issues

        - Update CI to support disk images, etc.
    - kas container
        - v4.3 : Docker image is reproducible
    - We need Debian snapshot, but performance issue there
    - How to resolve?
        - Cache
        - Aptly
        - …
- OSS-EU 2024 CFP (draft)

> Reproducible Builds makes supply chain secure by promising identical binaries (packages, VM/ISO/container images, etc.) are always generated from a specific source.
> For embedded devices, ready-to-install filesystem or disk images, which consist of bootloader, kernel, and root filesystem, are typically released through a certain image builder.
> An image builder that ensures reproducibility of output images should be a strong countermeasure against attacks to developing and uploading images in production releases as well as reference image distributions.
>
> The Civil Infrastructure Platform (CIP) project achieved reproducible builds for its reference OS images by enhancing the image builder isar-cip-core and related upstream projects.
> In this talk, Kazuhiro shows necessary functions in the image builder to make images reproducible, methods to detect and analyze reproducibility issues using tools like diffoscope, and concrete examples of detected issues and solutions, mentioning contributions to related communities so far.
> Additionally, it's evaluated how the image reproducibility works for device update scenario in terms of image size reduction.

    -

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)

deby

- (No update)

CIP Core Testing

- No OpenBlocks IoT device available in LAVA
    - AI: Enable OpenBlocks IoT in isar-cip-core & CI

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

- https://gitlab.com/cip-playground/debian-cve-checker
- Sample output (Excel)
- [02/13] Shall we remove this section as it's a completed one?
- AI(Toshiba): Move it to cip-core sub group
- [4/23] No update

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

-
- Renesas RZ/G2M
    - Enable secure boot
        - [4/23] No update
- Siemens M-COM
    - (Waiting for receiving the board)
    - [4/23] No update

wfx

- AI(Kazu): Consider creating a proposal to include wfx in the CIP project
    - At least for demonstration
    - Run tests regularly? (e.g. Run wfx server on AWS)

    - Just for Integration? Or Marketing?
- Other plans
    - Debian packaging?
        - https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1057366 / ITPed
        - Now building with go build

Secure update framework (TUF)

- Investigation for TUF implementations

Implementation	Description	Status

Notary project	• v1: https://github.com/notaryproject/notary
	  ◦ Complies with TUF
	  ◦ Development is still continued, but v2 is more active
	• v2: https://github.com/notaryproject/notation
	  ◦ Complies with OCI
	  ◦ Designed for containers
	  ◦ Seems there is consideration to implement as TUF, but no concrete activity yet
	• Overall, tends to be migrating to container specific
		No plan

RS-TUF	• Created with FastAPI & python-tuf • It seems to be a simple way to manage metadata • Very similar to the one implemented in the OSSJ demo	**Prototyping**

Uptane	• Originally to manage vehicle updates
	• Not a specific implementation but may be a reference for embedded devices
	  ◦ Configurable based on target systems
	• Two levels of image & metadata management
	  ◦ Manual part for clients
	  ◦ Fully automated part to manage devices
	• Support encryption in distributing images
		Investigating

- Connected to related OSS projects
    - TUF community
    - RS-TUF
    - SWUpdate
- (WIP) Prototyping CIP Core + SWUpdate + TUF example with RS-TUF
    - Server side (Docker Compose)
        - RS-TUF:
            - Manage metadata files
            - Shares metadata with the server through shared storage
        - Server (Built with FastAPI):

                - Allows clients to upload images and gets information about the updated images (hash, size, etc.)
                - Devices can download metadata and updated images via API
        - Device side
            - SWUpdate
            - swupdate_suricatta.lua
                - Polls the Server with tuf-client
                - If there is an available update, it downloads & installs it
                - suricatta uses tuf-client as a command-line tool
            - tuf-client (Made by go-tuf)
                - Go can be compiled and distributed to devices
                - Preparing dependencies in Python is troublesome
                - Refreshes metadata (& checks if there are update images) & verifies downloaded update images.
        - Status
            - Finish initial PoC
            - Updating cip-tuf-demo

Delta update support

- (WIP) Prototyping delta update methods for CIP Core image
    - [04/23] Patches (v3) sent to integrate Delta Update in isar-cip-core in the CIP mailing list. Link:https://lists.cip-project.org/g/cip-dev/message/15558
    - Feedback received from community is to create either a complete update file (.swu) or a delta update file depending on the user configuration.
- EOSS-US
    - https://sched.co/1aBFE
    - Another talk about delta (overview?) from Toradex

Test automation

LAVA software update test automation

- **[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.
- Planning: Create test results of SWUpdate/secure boot tests with SQUAD

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