CIVIL
INFRASTRUCTURE
PLATFORM

CIP Core regular meeting

- **Date: February 27th (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): Update WG wiki page
- Debian Extended LTS
    - 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
- 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

IEC-62443-4

- M-COM device shipment updates
    - Siemens shipped M-COM devices to BV, Toshiba India and Moxa
    - Delivery is expected by E/Feb (No updates just a guess) or earlier
        - BV confirmed two devices received
        - Siemens members checking the issues faced by Moxa
        - No further updates received from Siemens side
- BV meetings update (from CIP Core perspective)
    - SM-7: [Question] How to ensure the protection of the product or product update (patch) during design, implementation, testing, and release?
    - SM-9: What are the security requirements for externally provided components, who makes the decision to include external components in CIP, do we make some risk analysis if any by including such components in CIP?
        - Q. Examples of “external components”?
            - A. For CIP Core, non Debian components
        - Some examples
            - Local files in isar-cip-core (examples)
            - Files fetched from remote sites by isar-cip-core recipes
            - others?
    - Following requirements are approved by BV
        - SM-1-a to SM-1-f, SM-2, SM-3, SM-5, SM-6, SM-8, SM-10
            - It means no further updates/discussion required for these requirements

    - BV and SWG agreed to first completely finish IEC-62443-4-1 assessment then initiate 4-2 assessment
        - SWG will share the revised schedule for assessment for BV confirmation
    - Regarding essential package list decision for isar-cip core
        - SWG created complete list of packages isar-cip-core security image and test evidence availability in Debian CI and individual package upstream tests and it's available here
            - https://docs.google.com/spreadsheets/d/1rOHJUhUOa05Kkn4typfczSZTtKWc1YoL/edit#gid=32781124
            - Next step is to investigate packages where in both places (Debian CI and package upstream or salsa, column E & F) test are not available
            - SWG has also initiated discussion with the help of Neal if Alpha-Omega OpenSSF project can help to tests few debian packages specially from security perspective
- SWG has also contacted with few package maintainers where tests are not available or having some issues
- BV has requested to SWG to share user manual and hardware spec for M-COM device for SVV testing, waiting for updates from Siemens

- **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.
    - [02/27] 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 under Kazu-san's review.
        - https://gitlab.com/cip-project/cip-testing/cip-security-tests/-/merge_requests/15

Reproducible builds

CIP Reproducible build status

	Reproducible Build Status		
Target	**Raw contents**	**Filesystem Images**	**Disk Images**
QEMU AMD64	**Reproducible**	Not reproducible**	Not reproducible**
QEMU ARM64	**Reproducible**	Not reproducible**	Not reproducible**
QEMU ARMHF	**Reproducible**	Not reproducible**	Not reproducible**
BBB	**Reproducible**	Not reproducible**	Not reproducible**

* Currently patches for ext4 reproducibility are accepted by the OpenEmbedded Core community. ISAR repository needs to be updated to bring these changes.

** Filesystem images (squashfs) is not reproducible when generated on different days. Issue link: https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/94

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)	**Not 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)	**Not 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**)
  - [02/27] Currently investigating issue #94 in isar-cip-core regarding swu file reproducibility when created on different days: https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/94
    - squashfs images built on different days is not reproducible
    - [02/27] The issue is with the /etc/shadow file when the rootfs is generated on different days. Details in the above issue link.
    - [02/27] IMAGE_UUID was also reported to be changing when the images were built on different days. But based on current investigation, IMAGE_UUID is not changing between builds.

Disk images: (Completed)

- Artifacts built as bootable disk images with partition table included.
- Features enabled: Base + signed swupdate + secure boot + security configurations.
- CI pipeline: **In-Progress**
- 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

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)
  - swupdate: Use prebuilt version on sid
  - Changes to deploy .swu
  - add SWUpdate 2022.12
  - update ISAR to latest next for dh-compat improvements
  - Changes manage dpkg DB for RO rootfs
  - linux-cip: Update to 4.19.306-cip107
- 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

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
    - [Feb 27th] No update
- Siemens M-COM
  - (Waiting for receiving the board)
  - [Feb 27th] No update
- BBB
  - Confirm no BBB with the HS variant
    - There is no HS variant available in the market. Alternatively AM62x SOCs can be used for secure boot.
  - Stop further investigation for BBB to enable secure boot
    - No strong demand from members
    - SoC is already quite old, we should check other physical board with recent 64bit SoC

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

- (No update)
- (WIP) Improve implementation (of OSSJ demo) and documentation based on practical use cases, attack patterns, etc.
    - Planning to use RSTUF, see below
- (WIP) Investigation & prototyping for other TUF implementations
    - Notary
        - 2 versions are available.
            - V1: https://github.com/notaryproject/notary
            - V2: https://github.com/notaryproject/notation
        - The first complies with TUF; the second does not (complies w/ OCI). v2 focuses primarily on container management.
        - Additionally, v1 has not been discontinued, but v2 is being actively developed.
        - They are considering implementing TUF in v2, but it isn’t concrete.
    - RS-TUF
        - It is created with FastAPI & python-tuf.
        - It seems to be a simple way to manage metadata.
        - Very similar to the one implemented in the demo.
        - We are checking a few more specifics.
    - Uptane
        - This is an approach that uses TUF to manage vehicle updates.
        - This is not a specific implementation, but may be a reference for embedded devices.

Delta update support

- Aspects
    - Network traffic
    - Storage size for all update images
    - Flash life-time
    - Device side workload & required memory / storage while updates
    - Total update time
    - Offline update support
- (Done) Basic investigation of delta encodings
    - Ready-to-use methods:
        - librsync as rdiff handler

    - zchunk as delta update handler
  - Proc & Cons

	librsync (rdiff)	zchunk
Delta size	Large	Small
Delta management	Delta for each version combination or A/B synchronization required	Only chunks required
Device workload	Low	High
Update time	Short (but A/B sync needs multiple installations)	Long
Offline update	Feasible	Not feasible

  - zchunk looks more efficient from size perspective
  - Clarification & evaluation from other perspectives required
- (WIP) Prototyping delta update methods for CIP Core image
  - librsync (rdiff handler)
    - Verified delta update with local changes to recipes with some changes to round robin handler.
    - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/86
  - zchunk (delta update handler)
    - Lua handler is updated to support zchunk based delta handler. Changes are merged to swupdate-handler-roundrobin master branch
  - Siemens: Related proposal for EOSS US is being planned
    - Toshiba: Unfortunately it's hard to attend the EOSS in-person, but will contribute the activities to make the talk of delta update
  - [02/13] Verified applying Delta update with Secure boot enabled image for qemu-amd64 architecture and details of the verification is updated in the investigation document.
    - https://docs.google.com/presentation/d/16iMgqzKczvWTufkWF_EwzaUMNhsQAmoi/edit#slide=id.p1
  - [02/13] Issue regarding build failures in arm64/armhf when delta handler (zchunk) is enabled is resolved.
    - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/93
  - [02/27] Created a test branch with details of using Delta update for CIP members to try and verify.
    - Test branch: https://gitlab.com/cip-project/cip-core/isar-cip-core/-/tree/toshiba/delta-update-support?ref_type=heads
    - Currently working on improving the delta update recipes in the test branch linked above.

        - Also created an issue in isar-cip-core for initiating a discussion on integrating delta update in isar-cip-core. Link: https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/99
- Other plans
    - Evaluate delta size for multiple update patterns
    - Research to make delta size smaller
    - Evaluation from other aspects (workload, update time, offline update)
- Current investigation document which includes comparison, pros and cons of delta update support
    - https://docs.google.com/presentation/d/16iMgqzKczvWTufkWF_EwzaUMNhsQAmoi/edit#slide=id.p1

Test automation

LAVA software update test automation

- [02/13] Job definitions are prepared for software update (3 successful + 2 watchdog jobs), secure boot (3 jobs) and IEC Layer (3 jobs) under Chris's review.
- [02/13 Toshiba in discussion with CIP members for the approach to generate and upload .swu file in gitlab-ci. Prepared initial implementation and mentioned in this ticket.
    - Currently Toshiba is trying to understand about a much lighter method using ad-hoc jobs based on Jan's suggestion
    - **[02/27]** Patches (a) and (b) to upload .swu file and firmware binaries merged in isar-cip-core master branch. These artifacts can now be used in LAVA job definitions.
- [02/13] Toshiba proposed a method to trigger LAVA jobs for cip-core testing. Waiting for CIP members' opinions.
    - Kazu: linux-cip-ci is kernel specific, maybe should not be used for CIP Core testing. How about suggesting to create another project to store the job definitions for CIP Core? In that case, the script to submit jobs (currently in linux-cip-ci) should be put in a common place
    - **[02/27]** Chris suggested to initially create a repository under cip-playground to store cip-core LAVA jobs and it can be brought under cip-project/cip-testing in future after TSC's approval.
    - **[02/27]** Currently the submit script used in linux-cip-ci is more specific towards kernel testing in LAVA. Some functions in that script cannot be used to submit cip-core LAVA job due to significant format differences in the job definitions. So currently we can use a minimized version of that script in our new project with only necessary functions.
    - Kazu: First, let's create a tiny function for CIP core first, share it in cip-playground then get feedbacks from testing WG. Also check the necessity of sharing the commont scripts / data like

https://gitlab.com/cip-playground/cip-lava-job-submitter/-/blob/thond/lava.sh?ref_type=heads between kernel and CIP Core.

Other topics (not started yet)

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

Q&A or comments

- Dinesh (Do we plan to join next TUF community meeting)

Items that need approval by TSC voting members

- None