CIVIL INFRASTRUCTURE PLATFORM

CIP Core regular meeting

- **Date: June 4th (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**

	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 (rewrite) WG descriptions in CIP home page => Done**
- AI(Kazu): Update WG wiki page
  - [6/4] No update
- Debian Extended LTS
  - [6/4] 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(All): Enable OpenBlocks IoT in isar-cip-core & CI
  - AI(Toshiba/Siemens): Enable Siemens MCOM in isar-cip-core & CI
    - [6/4] See below
  - 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
            - [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
            - [05/21] Iwamatsu-san merged M-COM kernel config for 5.10 and has asked to share M-COM kernel config for kernel 6.1. I assume this work is in progress at Siemens side
            - Quirine shared MR for X86 generic kernel config and Chris confirmed on QEMU it can boot even kernel 6.1
                - https://gitlab.com/cip-project/cip-kernel/cip-kernel-config/-/merge_requests/92
                - Still other discussion and merging for other architectures in progress
            - [06/04] M-COM device booting confirmed with 6.1 merged defconfig, it's not clear whether there will be M-COM specific defconfigs
                - Also discussion in progress with Benjamin if there are any M-COM specific defconfigs
                - Now testing with isar-cip-core master branch, without any custom patches
                - The image without SWUpdate and secure boot boots successfully
- debian-cve-checker
    - AI(Toshiba): Move it to cip-core sub group
    - [6/4] 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 (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
- [5/21] No update

IEC-62443-4

- Verified 6.1 kernel booting on M-COM with minimal image
- Security image testing on M-COM
    - Created SWUpdate image using kernel 5.10 and while testing, reboot issue is observed due to WDAT timer expiration
        - Discussing further with Benjamin how to enable WDAT on M-COM
            - Rollback is not important for IEC assessment so it can be a low priority task
                - (of course, it’s quite important for products)
    - For verifying secure boot, waiting to receive detailed steps and how to use TPM and key enrollment etc
        - Document is already present
        - Device specific details should not be required for MCOM
    - Next step: verify SWUpdate with kernel 6.1
- Bug tracking locations to be added in IEC documents
    - https://gitlab.com/groups/cip-project/cip-kernel/-/issues
    - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues
    - Can Security WG add those links to IEC document?
        - Kazu: No concern
    - Release checklist

        - Dinesh: Issues that should be resolved by each release also in the GitLab issues?
        - **Will discuss in the next meeting**
- 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
        - [**05/21**] SWG had a discussion about this topic with BV, BV suggested to consider doing risk assessment for packages having no tests and proceed from IEC assessment perspective, meanwhile SWG can continue to investigate how to add tests for required packages
        - [**06/04**] No updates, need to start risk assessment for the packages having no tests
- Integration of duplicity package to isar-cip-core for IEC layer
    - Work in progress to include duplicity in the IEC layer (to fulfill IEC 62443-4-2 CR 7.3 requirement) .
    - Based on suggestions provided by Jan in this discussion , recipes shall be implemented to set up a scheduled service for remote backup along with configuration of backup sources during the image build.
    - AI(Dinesh): Share the information about why duplicity is preferred for IEC
    - **[06/04]** Duplicity is chosen by SWG because it internally supports encrypted, incremental local and remote backup, integrity verification before restore and also data restoration (IEC 62443-4-2 CR 7.3, 7.3 RE(1), 7.4). Creating recipes which do scheduled backup using a service is in progress.
- Update on security issues reported by Jan for next isar-cip-core release
    - Detailed discussion in gitlab

                - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/108
                - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/107
                - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/105
            - Syslog-ng package removed from isar-cip-core security image
                - Alternate option is used as systemd-journal
            - Tpm2-abrmd package removed
                - Not clear what's the alternate option
            - Fail2ban dependency changed to systemd-journal
        - It's also found the networking services start late even in isar-cip-core minimal image in bookworm whereas this issue is not found in bullseye
- Review all IEC layer packages with CIP Core members as the current list was investigated by SWG members when Debian version was buster
    - To align with CIP Core members, it's better to review entire IEC layer package list
    - Also decide some process in case of any additional packages required how it should be decided
    - There can be multiple factors to make decision e.g.
        - Keep minimal packages as part of IEC layer as more packages adds more security issues and increases maintenance effort
        - Add all required packages to meet IEC requirements, it will help to meet maximum IEC-62443-4-2 requirements
        - Consideration of priority for specific use cases like IoT device, network device and any embedded devices
    - Past investigation data from SWG
        - https://docs.google.com/spreadsheets/d/1y3DIozi55VgvCADDTnqtVA6k3mT-4SAS/edit#gid=976172816
        - https://docs.google.com/spreadsheets/d/14pTlli3nf1GX37V2R0hl54wzcauC_ZW2/edit#gid=1649837888
    - Use cases for each IEC requirement should be clarified before adding packages
        - Dinesh: Security WG will discuss and make use cases clear, then conclude this topic
        - Dinesh: Any other categories that CIP members want to apply CIP Core than embedded IoT devices?
- **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.
    - **[05/21]** Created a new issue in Gitlab to continue discussion. Quirin suggested a workaround to handle the Syslog issue. A bug shall be reported to syslog-ng Debian package.

    - **[06/04]** syslog-ng-core, and tpm2-abrmd packages are removed from security target.
    - **[06/04]** IEC layer tests which require syslog data will now be modified to use journal logs. MR creation is in progress.

Reproducible builds

- WG will have meeting with RB project members on June 25th 22:00 JST
- Reproducibility issues in generating CIP Core image
    - **[06/04]** Currently after taking the upstream fixes from OE-Core, /home partition is now reproducible. But the /var partition and the ext4 partition in the BBB image are still not reproducible.
        - /var, BBB => wic library (OE-Core)
        - No difference in files, maybe in FS metadata etc.
        - URL:https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/75
        - /var: not complicated
        - BBB: Need investigation
    - **[06/04]** The /var partition reproducibility issue is due to missed handling for reproducibility in wic when an empty ext4 partition is deployed (As we do in CIP currently)
        - Rootfs hook seems not be run if the partition is empty
    - **[06/04]** The ext4 image for qemu base targets (without swupdate support) are also not reproducible.
        - image-type.bbclass is isar
        - URL:https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/74
        - Need investigation
- (WIP) Updating CI to check reproducibility of disk (wic) images
    - Waiting for isar-cip-core pulls the fixes
    - [05/21] The following patches were sent to OE-Core and is yet to be pulled by ISAR:
        - https://patchwork.yoctoproject.org/project/oe-core/patch/20231218043030.32027-1-venkata.pyla@toshiba-tsip.com/
        - https://github.com/openembedded/openembedded-core/commit/150e079589e207fe174d2dceb40cd8f3d3972c5a
        - NOTE: The above mentioned patches are already available in isar and are also currently referenced and used by isar-cip-core.
- ~~(Done) 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)
        - [06/04] The changes to enable building against snapshots when requested is available in the master branch of isar-cip-core.

        - No additional setting to do in isar-cip-core than setting the flag (ISAR_USE_APT_SNAPSHOT = 1)
            - Defined in kas/opt/reproducible.yml
    - [6/4] Tested

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?
- Cip Core waiting for https://patchwork.isar-build.org/project/isar/list/?series=1189

deby

- (No update)

CIP Core Testing

- AI(All): Enable OpenBlocks IoT in isar-cip-core & CI
    - Merged x86 generic kernel configs are ready, we can proceed by updating recipes? => check with Iwamatsu-san
- 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

-
- 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
    - (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)
    - Others
        - 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-**6** : Finish step 1 implementation
        - 2024-9 : Finish step 2 implementation & demo
    - Status
        - **[06/04 Adithya]** Completed integrating RS-TUF server components in cip-tuf-demo. Verified changes locally.
        - **[06/04 Adithya]** Replaced python tuf-client with go based implementation. Verified changes locally.
            - Enable build of go based tuf-client with recipes in isar build system.
            - Currently, the recipe relies on vendoring the go build dependencies. Could be updated for a better approach.
            - FYI: Having a TUF client function in SWUpdate itself from security perspective, suggested by the maintainer
            - Kazu:
- 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 and additional scenarios
    - **[06/04]** Verifying update with backend (wfx). Faced an issue with device rebooting unexpectedly before the Activation stage.
    - **[06/04]** Raised this as an issue in SWUpdate mailing list. https://groups.google.com/g/swupdate/c/wJ6g5lajuYw
    - **[06/04]** Christian has already sent a patch to fix the issue. https://groups.google.com/g/swupdate/c/ELPp5c0kWrI

Test automation with LAVA

- Milestones
    - 2024-6 : Finish cip-core-ci implementation for SWUpdate testing and enable CI
- Status:
- **[05/21]** 3 separate jobs shall be added to test 3 functionalities separately as mentioned in this commit.
- **[05/21]** Requested Chris to enable multiple QEMU devices in CIP LAVA Lab with the device dictionary changes required to boot CIP security image in LAVA which helps in reducing test jobs runtime because of parallelization.
    - Cannot run tests in parallel unless there are available GitLab runners, etc.
- **[05/21]** Group and projects to host CIP Core test results on SQUAD are created by Chris.
- **[05/21]** Changes to test SQUAD job submission are made in this commit . Requested Chris to provide project slug and group slug details since they are required while calling watch job API.
- **[06/04]** Patches to trigger swupdate, secure boot and IEC layer testing LAVA jobs were shared for review. Jan suggested creating a README document to explain how the job definitions are created and functionalities are tested. Rework is 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