CIVIL INFRASTRUCTURE PLATFORM

CIP Core regular meeting

- **Date: July 16th (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 WG wiki page
  - [7/16] WIP: Adding RB introduction page
- Debian Extended LTS
  - [7/16] 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
    - Plat'Home will try to install & boot the generic x86 image
      - [7/16] No update (by minmin)
- IEC 62443-4
  - ~~AI(Dinesh): Do survey to check if any members have requirements / use cases to backup/restore feature~~
    - [7/16] No use cases are shared by anyone for the survey conducted hence SWG concluded to consider CIP reference images does not support backup/restore, CIP users can add required packages/services to support specific use cases.
  - ~~AI(Toshiba): Fix the commit of cip-security-tests used in isar-cip-core~~
    - Done: https://gitlab.com/cip-project/cip-core/isar-cip-core/-/commit/e40f61ef7753b9e99e4342b385359624cad96bea

- CVE checker
    - ~~AI(Toshiba): Move it to cip-core sub group~~ => Done
- 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

IEC-62443-4

- 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)
            - **[**6/18**]** Benjamin mentioned in SWG meeting he will get WDAT information on M-COM from Siemens members and share
            - [7/02] Waiting to receive any updates from benjamin
            - **[7/16] No updates**

    - (Done) Secure boot verification on M-COM
        - **[**6/18**]** Based on discussion with Benjamin and by following steps from README we tried to enroll keys but device is unable to come out of setup mode, investigating further and also will share details of this issue with all members
            - Deleted all secure boot keys
            - Inject new secure boot keys using KeyTool
            - Secure boot has not been enabled even after update the keys
        - [7/02] Secure Boot is verified on M-COM device and injected keys by following steps mentioned in the README
            - Can we discuss the feedback from Jan for the README shared in ML?
            - No need to add MCOM specific steps into (common) README file
        - [7/16] Nothing pending now, once all README patches are merged in master branch, SWG will ask BV to verify security images booting and secure boot is enabled to complete setup at BV side
    - (Done) Software Update verification on M-COM
        - Complete Software update with CIP kernel 6.1 verified
        - Delta software update with rdiff also verified with kernel 6.1
- Support of backup/restore in isar-cip-core for IEC layer
    - **[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.
    - [**06/18**] Discussion in gitlab 110 initiated but we are waiting to get feedback from Stefan.
        - Any use cases from members for the backup/restore feature?
        - What is the target of backup/restore?
        - Let's clarify them to achieve the IEC requirement as "generic" feature
    - [**07/02]** Stefan's suggestion regarding devices with and without state.
        - After discussing the backup/restore requirement in the SWG meeting, it was decided to have a basic implementation using rsync in the IEC layer.
        - Steps to perform automated remote backups, integrity checks, and restoration are mentioned in this issue.
        - Jan suggested getting pratical input from a use case where backup from the device is actually implemented.
            - According to IEC 62443-4-2 7.3, 7.3 RE(1) and 7.4 requirements expect for automated remote backups.

                - This will be device specific (state/without state) and if the user wants this feature then there are steps such as adding SSH keys to their remote server for easy remote backups.
                - If the device is stateless then this feature is not required.
            - Features added into isar-cip-core should have specific requirements and use cases that are not just for certification
            - **AI(Dinesh)**: Do survey to check if any members have related requirements / use cases
        - [**07/16**] No responses for backup & restore use-cases received during survey.
            - Hence it is decided in the SWG meeting to document that “CIP reference images do not support backup/restore functionality from the platform side, hence all CIP images will be stateless”.
            - SWG members will discuss it further with BV if this is sufficient or anything else required during 4-2 assessment
- 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/14pTlli3nf1GX37V2R0hI54wzcauC_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?
    - [06/18] No update
    - [07/02] Sorry still this is in progress, all SWG members did not join the last meeting.
    - **[07/16]** There are some discrepancy in requirement IDs mentioned in the BV provided sheet, SWG will clarify with BV and proceed to create final list

        - https://docs.google.com/spreadsheets/d/1Ihrry5koqqxa8AVuv8UITJ6nAgXfhpzU/edit?gid=986512146#gid=986512146
- **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.
    - **[06/18]** MR review is in progress
    - **[07/02]** MR review by Stefan is still in progress.
    - Jan: IEC tests are now failing
        - They will be passed once the MR above is merged
        - In addition, we need to fix the commit of cip-security-tests used in isar-cip-core
            - **AI(Toshiba)**: Fix the commit
    - [**07/16**] MR 18 and MR 19 are merged to master on 15th July.
        - With these changes, 42/43 test cases will pass.
        - TC_CR1.11_2 test case is failing irregularly. Investigation in progress.
            - Account locking during incorrect remote login attempts is verified as part of TC_CR1.11_2 test case.
            - It is configured to lock the account for 10 seconds after a single incorrect login attempt.
            - After an incorrect login attempt, a login attempt is made again to verify whether the account is locked or not.
- CIP Core test report generation (for IEC)
    - **[07/16]** Here is a PDF report generated from an html report from SQUAD
    - WIP: Toshiba is able to get IEC layer test reports from SQUAD but there are slight mismatches in the report Investigation in progress.
    - WIP: Sietze suggested generating PDF reports for CIP Kernel and CIP Core in CI instead of manual approach.

Reproducible builds

- Actions from RB team meeting
    - Resolve diffoscope performance issues
        - **[07/16]** WG shared CIP core security images with the RB team on 8-July in order to help them debug the diffoscope performance issues with larger images. No update from RB team yet.

    - 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
        - **[07/16]** Shared the backported patch to isar, awaiting feedback from maintainer.
    - (2) rootfs ext4 formatted partition size sometime varies
        - Blocks occupied in disk change in each build
        - rootfs contents are identical
        - **[07/16]** 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
        - **[07/16]** Preparing a patch to calculate the rootfs size similar to how its done in OE-Core
    - (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 June 4th
    - doc/README.secureboot.md: Add steps to inject UEFI keys from KeyTool.efi
    - tests: Pin revision of cip-security-tests
    - Kernel updates
- Recent releases
    - v1.4 -rc1 (May 31st)
    - **v1.4 (June 25th)**

deby

- (No update)

CIP Core Testing

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

CVE Checker

- https://gitlab.com/cip-project/cip-core/debian-cve-checker
    - **[7/16]** Moved to cip-core sub group
- Sample output (Excel)
- **[7/16]** (Done) MR to build docker images with cve_checker.py and dependencies is merged
- **[7/16]** (WIP) As Debian buster moved to ELTS, Toshiba is working to change the source URL to freexian in case the suite is buster
    - Finally a patch shall be sent to isar-cip-core to update image reference in cve-checks job
    - Related issue: https://gitlab.com/cip-project/cip-core/debian-cve-checker/-/issues/1

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-EU
    - WIP: See IEC section above

wfx

- [7/16] Checking ways to publish a new CIP site (e.g. wfx.cipatform.org)
- 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
        - **[07/16]** 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.

- Other topics
    - Debian packaging? (Currently building with go build)
        - https://bugs.debian.org/cgi-bin/bugreport.cgi?bug=1057366 / ITPed

Secure update framework (TUF)

- (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 (**Step-1**)
        - Completed integrating RS-TUF server components in cip-tuf-demo. Verified changes locally.
        - 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
        - Four MR's are created for Step-1 integration of RSTUF
            - All MR's merged
                - https://gitlab.com/cip-playground/cip-tuf-demo/-/merge_requests/2
                - https://gitlab.com/cip-playground/cip-tuf-demo/-/merge_requests/3
                - https://gitlab.com/cip-playground/cip-tuf-demo/-/merge_requests/4
                - https://gitlab.com/cip-playground/cip-tuf-demo/-/merge_requests/5
            - **[07/16]** README update in-progress to mention dependency packages needed in the host system to run the demo and address few other remarks.

        - Issue: https://gitlab.com/cip-playground/cip-tuf-demo/-/issues/?sort=created_date&state=opened&first_page_size=50
    - Details of Step-2 plans is being prepared, would be shared in the next meeting
- Others
    - Verification with delta update
    - Uptane evaluation

Delta update support

- Milestones
    - 2024-5 : Finish isar-cip-core integration (Done)
    - 2024-8: Verify typical use cases including backend (Done)
    - 2024-9 : Demo
- Minor topics
    - Zchunk with MCOM

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
- [**07/16**] No updates because the M-COM device has not been added to CIP LAVA Lab yet.

Other topics (not started yet)

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

Open Source Summit Europe 2024 Demo preparation

-

Q&A or comments

- [Dinesh] Do we have any idea when M-COM device will be added in the CIP LAVA Lab?

    - Let’s check in today’s TSC meeting

Items that need approval by TSC voting members

- None