CIVIL INFRASTRUCTURE PLATFORM

CIP Core regular meeting

- **Date: March 28th (Tuesday), 2023**
- 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)** **Dinesh Kumar** **Venkata Pyla** Shivanand Kunijadar Tho Nguyen Dat

Discussion

Action items updates

- AI(Kazu): Update WG wiki page => Started
  - Need to add the following information that was discussed in CIP Core
  - In CIP, some development works (e.g. adding autopkgtest) are on-going but they (mostly?) target on bullseye(stable) or older
  - CIP Core should have clear policies about which Debian release that CIP mainly develops new features
    - Development: sid (= testing until soft freeze)
    - Maintenance: stable or older
  - This would prevent CIP from having their own infrastructure (=additional efforts) to maintain their custom (backported) features and would make more chances to discuss / contribute with/to upstream (Debian)
- Debian Extended LTS
  - AI(Kazu): Package proposal for Debian jessie
    - ~~WIP: Have an issue in script~~ => Solved, creating the proposal
    - **... but LTS defines the format of package list. It might be better to revise cip-pkglist scripts to meet the format**
  - ~~AI(Kazu): Start discussion about kernel collaboration in cip-members~~
    - **Done**
- IEC-62443-4-1
  - AI(Kazu): Create the package proposal for bullseye minimal packages
    - ~~WIP: Have an issue in script~~ => Solved, creating the proposal
- Isar-cip-core
  -
- CIP Core testing
  - No OpenBlocks IoT device available in LAVA
    - ...

        - (as of 2023-02-28) No major progress has been made since the last meeting.
            - I have not received the results yet, although I have received a response from Iwamatsu-san saying that he will check on it.
            - A patch for 4.19 is not ready yet.
            - Target kernel versions
                - 4.19
                    - Need some patches to fix the USB related issues above
                    - Plat'form may suggest patches for the issue?
                - 5.10
                    - Looks working in Plat'home's local environment, waiting for response from Iwamatsu-san
                    - Recipes for isar-cip-core could be implemented
        - (as of 2023-03-14) I prepared a patch for Iwamatsu-san. I was informed by Iwamatsu-san that this is due to the fact that this change is not included in 4.19.
            - https://gitlab.com/cip-project/cip-kernel/linux-cip/-/commit/cdfee5623290bc893f595636b44fa28e8207c5b3
            - However, this change cannot be adapted to 4.19 as it is, and Iwamatsu-san is currently considering this change.
        - (as of 2023-03-28) No update.
- cip-core-sec
    - AI(Toshiba): Add improvements to solve some issues and make the project official (move to cip-project)
    - AI(Toshiba): Update the ISAR gitlab-ci integration branch
- SWG AI
    - CIP Core release process
        - ~~**AI(Kazu): Create a thread in CIP ML**~~ **=> The versioning rule decided**
    - Discussion with BV
        - Meeting with BV and CIP members planned today for discussion about contract signing and clarifications from both sides
    - Updates from Siemens
        - Siemens members have finalized device called M-Com X86 to be shared with CIP members for testing and development
            - It already supports CIP Kernel 5.10
        - Available boards: at least 3 for CI (LAVA), and 1 for IEC work
        - Updates from SWG meeting 13/Mar
            - One device would be needed asap
            - Two devices can be shared late

        - Confirmation from Bosch
        - BV requires three devices for testing
    - Is there any timeline by when isar-cip-core images will be supported on M-Com X86 ?
        - Jan would like to continue support this board for bullseye as well
        - Officially, CIP Core can release bookworm based images after Debian bookworm released (around July-Sep)
    - Are the recent TPM commits in isar-cip-core are related to support secure storage in M-Com X86?
        - TPM for QEMU is implemented
        - It should also work for M-Com
- Discuss with Renesas about supporting isar-cip-core images, SWUpdate and Secure boot
    - Kent mentioned in SWG meeting, Mr. Hung will update about isar-cip-core support on G2M and how Secure storage is accessed in G2M
    - By when Renesas plans to support SWUpdate & SB on G2M using isar-cip-core images ?
    - Who can provide details on how secure storage will be supported using generic solutions?
    - The topic was discussed, Renesas members are still discussing, points mentioned by Renesas in SWG
        - Ideally it should be handled by SWG members
        - Renesas members don't have experience working on isar-cip-core
        - RZ/G2M has capability to support OPTEE
        - Overall, still Renesas members discussing about SWG queries how best Renesas can support
        - Renesas: FYI, Renesas BSP is public at https://github.com/renesas-rz/meta-renesas. Currently we already use Optee for secure boot https://github.com/renesas-rz/meta-renesas/tree/dunfell/rz/recipes-common/recipes-bsp. We are checking in our side whether this is match with above questions.
    - Renesas: internally discussing, will reply around 1-2 weeks later
    - **On G2M device**
        - IEC tests with isar-cip-core image are passing? => Not check yet
        - SWUpdate support? Or someone enabling this? => Hung-san will check the status
          –> SWUpdate support Renesas G2M device. But look like it is too old, so cannot build now.

          $ cd isar-cip-core

$ git checkout cip-sw-updates/swupdate
$ ls board*
board-bbb.yml board-qemu-amd64.yml
board-simatic-ipc227e.yml
board-iwg20m.yml **board-rzg2m.yml**
$ ./kas-container build kas.yml:board-rzg2m.yml
....
addtask rootfs before do_build
^

SyntaxError: invalid syntax

- AI(Kazu): Share info how to build image with SWUpdate for G2M

- Secure storage support?
  - Secure storage for ARM has not integrated to isar-cip-core yet
    - 28/03:
      Secure storage is supported by Renesas proprietary software for G2M. NDA required for distribution of Renesas proprietary software and documentation.
  - What kind of hardware support is provided in G2M?
    - 28/03:
      G2M and Renesas proprietary software pre-assessed by CSSC, ISASecure accredited certification body, as following results.
  - For example, if CIP members (non Renesas members) want to use / evaluate secure storage features on G2M, does the member need NDA?
    - AI(Kent): Confirm if it's required or not (maybe not required)
    - If not required, we can check more details about drivers below as the next step
  - Two type of drivers are provided (proprietary)
    - Linux kernel driver
    - OP-TEE driver

Requirements		Results of Evaluation
FR 1: Identification and authentication control		
CR 1.5		
RE (1)	Hardware security for authenticators	Supported
CR 1.8	Public key infrastructure certificates	Supported
CR 1.9	Strength of public key-based authentication	Partially supported
RE (1)	Hardware security for public key-based authentication	Supported
CR 1.14	Strength of symmetric key-based authentication	Partially supported
RE (1)	Hardware security for symmetric key-based authentication	Supported
FR 2: Use control		
FR 3: System integrity		
CR 3.1	Communication integrity	Supported
RE (1)	Communication authentication	Supported
CR 3.5	Input validation	Partially supported

FR 4: Data confidentiality		
CR 4.1	Information confidentiality	Supported
CR 4.2	Information persistence	Supported
CR 4.3	Use of cryptography	Supported
FR 5: Restricted data flow		
FR 6: Timely response to events		
FR 7: Resource availability		
CR 7.4	Control system recovery and reconstitution	Partially supported
CR 7.6	Network and security configuration settings	Partially supported
Software application requirements		
Embedded device requirements		
EDR 3.10	Support for updates	Supported
RE (1)	Update authenticity and integrity	Supported
EDR 3.11	Physical tamper resistance and detection	Supported
EDR 3.12	Provisioning product supplier roots of trust	Supported
EDR 3.14	Integrity of the boot process	Supported
RE (1)	Authenticity of the boot process	Supported
Host device requirements		
HDR 3.10	Support for updates	Supported
RE (1)	Update authenticity and integrity	Supported
HDR 3.11	Physical tamper resistance and detection	Supported
HDR 3.12	Provisioning product supplier roots of trust	Supported
HDR 3.14	Integrity of the boot process	Supported
RE (1)	Authenticity of the boot process	Supported
Network device requirements		
NDR 3.10	Support for updates	Supported
RE (1)	Update authenticity and integrity	Supported
NDR 3.11	Physical tamper resistance and detection	Supported
NDR 3.12	Provisioning product supplier roots of trust	Supported
NDR 3.14	Integrity of the boot process	Supported
RE (1)	Authenticity of the boot process	Supported

    - Also, need to check the results of test cases in the IEC layer on ARM device (if RZ/G2M will be selected)
    - Moxa members checking failed tests on QEMU ARM64

Debian LTS / Extended LTS

- **The query from Freexian (Thorsten): Debian 10 buster package list**
    - Current situation in CIP

        - We only have a package list for buster that includes packages for the minimu base system (installed by debootstrap minbase): https://gitlab.com/cip-project/cip-core/cip-pkglist/-/blob/master/pkglist_buster.yml
        - No additional proposal from other WG (e.g. Security WG)
    - Plan: Core WG will provide the minimum package list above
    - Renesas: sorry, Renesas intend to submit our proposal for list of packages. Is it possible now, or too late? (if not, when is the deadline?) The list is not decided yet, but at least we intend to add packages related to security, with openssl at highest priority.
        - Creating the package list. it will take around 2 weeks?
        - Please share the package list once decided (ASAP) in cip-members
        - Feb.28th Fujita-san shared the package list, Core WG needs to fix the issue in cip-pkglist above first
        - Kazu: The problems in scripts has been fixed
        - AI(Hung-san): Check the current status in Renesas
          –> Confirmed that it is possible to run on Debian (although it is quite difficult to run on Ubuntu). Renesas can send the proposal soon.
- AI(Kazu): Package proposal for Debian jessie
    - WIP: Create “pkglist_jessie.yml” like buster then send the proposal
- The collaboration with ELTS in long-term supported kernel
    - Discussion with Freexian is on-going, but in not in ML

IEC-62443-4-1 requirements

- Review CIP requirements
    - If there are any CIP Core specific requirements, please share
        - https://docs.google.com/document/d/16dX-3coBeZonPGYgsPIOyniT3XYJcbNUu6RcOmrWkAw/edit
        - Markup document created and added
            - https://gitlab.com/cip-project/cip-documents/-/blob/master/process/CIP_requirements.md
- CIP Secure Storage
    - Stefan: For x86 based devices TPM based secure storage solution to be supported, more details to be discussed when available
    - https://docs.google.com/document/d/1sMeKBi11SJr2TpWP4b6EQKJGneMMjE-zPZIcHqUhvbA/edit
- CIP Security hardening document
    - Following MR merged, no other pending items as of now
        - https://gitlab.com/cip-project/cip-documents/-/merge_requests/31
- Add data encryption packages in isar-cip-core
    - No update
    - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/issues/29

    - Patches for adding package are in local branch but they are for ARM64 architecture
        - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/blob/2de2aaa5331b2094137779c4375ff877394415c9/doc/README.information-confidentiality.md
- SWG Proposal for final CIP IEC-62443 assessment
    - https://docs.google.com/presentation/d/1UXIi-Og-W88cJmnAd6gMowUn-9-kgUTP/edit#slide=id.p1
    - Siemens to confirm whether they plan to make SIMATIC IPC227G as CIP reference hardware in near future
    - Don't need to wait for Siemens decision about IPC227G
    - Another candidate would be RZ/G2M HopeRun HiHope (Armv8), but some features like SWUpdate, secure boot, has not been implemented / evaluated yet using CIP Core
- AI(Kazu): Create the package proposal for bullseye minimal packages
- CIP Core release image and release process
    - Requirements:
        - CIP Core image is required for running tests and producing evidence
        - The versions of CIP Core (and CIP kernel) are required for the final assessment certificate
        - CIP Core images should be released after security related issues are resolved
        - Define a procedure for testing security patches to make sure they fix the issue and don't introduce new ones
    - Related conversation
    - The current idea
        - When: Regularly releases just after Debian point release (e.g. 11.1, 11.2...)
        - What:
            - Recipes
            - ~~Images for each CIP reference hardware~~
                - Need to provide information of packages (i.e. package repository snapshot) if we deliver the images
            - Test results
            - Security reports (by cip-core-sec)
    - **SWG: Needs to define "version"**
        - Candidates
            - Date (e.g. 20230131)
            - x.y (e.g. 1.2)
            - Include Debian release: 1.2-11.6
            - Plan

            - Keep supporting multiple Debian releases in one branch (at the moment)
        - When the versioning needs to be decided?
            - SWG: In 2-3 months
        - After stable (oldstable, LTS, ...), when should CIP Core create release?
    - ~~AI(Kazu): Create a thread in CIP ML~~
    - **Use semantic versioning style: x.y.z**
        - x : All other significant changes than y and z
        - y : Incremented for each Debian point release
        - z : Incremented only when critical bugs are fixed
    - v1.0-rc1 tag is registered
        - https://gitlab.com/cip-project/cip-core/isar-cip-core/-/tags/v1.0-rc1

Reproducible builds

- Open issues
    - #54 [Software update image is not reproducible] - Open
        - (An image that includes SWUpdate package and related settings)
        - Sent patch to fix this issue in ISAR
        - No update
    - #56 [vmlinux is not reproducibly built in arm[,64] architectures] - Open
        - Reported issue in upstream (ISAR)
        - No update.
    - #58 Diffoscope tool could not verify disk images with partitions - Open
        - Sent query in reproducible-build community
        - No update

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/
- Updates
    - initramfs-crypt-hook: Add clevis for buster and bullseye
    - Enable ccache
    - linux-cip: Bump cip-kernel-config revision
    - kconfig: Allow to select encryption also for qemu-arm and qemu-arm64
    - start-qemu: Add TPM support also for arm and arm64
- Regarding CIP Core releases
    - It's now ready to make a release once the version name is decided

        - AI(Dinesh): Create a discussion in cip-dev about how to test security images
            - See “Query from Chris in ML”
- WIP: Patch series to build a QEMU setup which uses OP-TEE to use RPBM (Replay protected memory) of an EMMC for a secure storage are under review
    - QEMU: Require more engineering efforts to use the emulated functions
    - Does Renesas reference H/W have required capability? (OP-TEE, RPBM)
        - AI(Dinesh): Ask in Security WG
            - Yes, confirmed by Renesas.

deby

- (No update)

CIP Core Testing

- deby has the copy of linux-cip-ci's LAVA functions
    - (No update)
    - Plan: Create a separated repository to provide the LAVA functions => Other projects like linux-cip-ci, deby (and isar-cip-core?) reuse the repository
    - Created the draft project in playground
    - Implemented the draft and validating
- No OpenBlocks IoT device available in LAVA
    - The recipes for the device have been implemented in development branch and the OS images (kernel & rootfs) are built by CI
    - AI(Plat’Home): Update kernel configs
- Query from Chris in ML
    - If we have multiple versions of cip-core - which do we use for kernel testing?
        - If it’s v1.0 => Kernel testing only needs to focus on the latest version as long as the required Debian release is supported in it
        - If it’s flavor (e.g. minimum, security) => Currently, minimum images are used, adding extra features may not affect the test results
- Question from CB
    - How are we testing metadata? (e.g. static checks)

cip-core-sec

- (No update)
- AI(Toshiba): Add improvements to solve some issues and make the project official (move to cip-project)
- AI(Toshiba): Update the ISAR gitlab-ci integration branch

RISC-V Investigation

- "qemu-riscv64" image generation is supported in isar-cip-core master
  - Used to test CIP kernel with KernelCI
  - This is an exceptional target and not in WG's maintenance scope in official because it's based on Debian riscv64 packages in sid-ports which are not included in Debian official release (yet)

Software Updates WG

- Related updates in isar-cip-core
  -
- Support ARM targets
  - Supporting physical ARM64 boards?
    - Toshiba: MPSoC ZCU102 is a preferred option, but no requirement at the moment
  - Any boards that can be used to implement secure boot & secure storage?
    - CyberTrust (MPSoC ZCU102): No requirement, not sure about H/W features
    - Renesas: No requirement
  - Kazu: Q. Is it mandatory to support and test SWUpdate on the reference hardware (if it's ARM based) selected for IEC?
    - For SL2, Yes. It's better to ask Renesas members to check the capability / development / evaluation in advance if they want to select their board for IEC certification
- Request(Jan): Support data encryption (secure storage)
  - Pre-condition for security WG activities
  - AI(SWG): Discuss about requirements about secure storage
    - Currently lacking contribution in SWG to take up the pending work items
  - We'd like to have some common parts to support the feature among the multiple targets (in isar-cip-core)
  - Targets
    - QEMU (ARM): WIP
    - QEMU x86 : WIP*
      - TPM emulation configuration required
    - Physical boards
- SystemReady (from ETSC meeting on 2022-04-04)
  - Jan had a discussion with ARM
  - If the interface is very well implemented, it make simplify our implementation
    - IoT profile
  - CIP members have interest on this, but the details need to be checked
  - Related to SWUpdate/secure boot story

    - Clarify and share the basic features, check how it's related to CIP members' use cases
    - SystemReady is targeting on ARM
        - RISC-V is not included

SBOM support proposal from Siemens

- No updates
- We have to continue to discuss this topic further with CIP members as it's going to be one of the legal requirements in future globally, so addressing this topic is important
    - Related thread: "[cip-members] SBOM (Software Bill of Material) proposal"
- Following proposal was made by Stefan from Siemens to discuss possibility of supporting SBOM by reusing Debian packages
- Proposal
    - New legislation in the US and Europe will lead to SBOM (Software Bill of Material) mandates. Currently there are several competing standards (see https://www.linux.com/news/generating-a-software-bill-of-materials-sbom-with-open-source-standards-and-tooling/)
    - **Decision needed**: How does the CIP project want to communicate SBOM information to their users? This needs to be coordinated with the core-team.
    - **Suggestion**: Adopt the CycloneDX standard which is well established. Tools exist to create SBOM automatically for Debian (e.g. https://github.com/CycloneDX/cyclonedx-linux-generator)
        - CycloneDX can be used to collect information like below
            - All installed component types e.g. app, library, container etc
            - Known Vulnerabilities
            - Integrity verification
            - Authenticity of each component by digital signature
            - License compliance
            - Dependency graph
            - Many more... refer [1]
    - **References**
        - **[1]** https://cyclonedx.org/use-cases/
        - [2] https://cyclonedx.org/tool-center/

Q&A or comments

- **Can we support changelog for isar-cip-core meta-data?**

        - This will help in maintaining certification over period of time e.g. after certain period CB can audit changes and confirm to whether to renew certification or not
- Shall we create a common file as “Release_and Version” to document about the release process, frequency and version change process as agreed in the mailing list?
-

Items that need approval by TSC voting members

- None