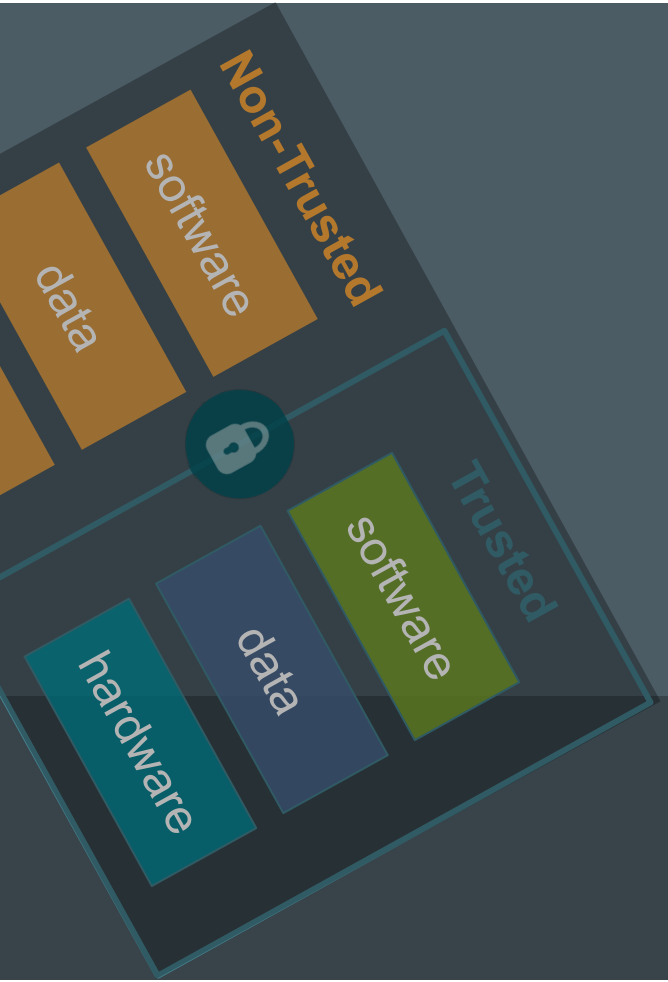


Open Source Secure World Software

Trusted Firmware Governing Board Meeting

13 July, 2022

HOSTED BY:

Linaro

Open CI Updates

Open CI Updates

Progress - June

- Production & Stage Update - migration of Jenkins, dependent plugins and OS.
- Mbed TLS addressing issues with windows platform
- MISRA Planning complete, M1 Infrastructure setup underway.
- Advanced PSA Compliance Test integration, FirmwareFramework completed, additional test tuning
- Advanced Code Coverage integration, debugging issues and ongoing maintenance.

Active Issues:

- Active Hardware Issues
  - Second rack is needed to install STM32MP15 boards, Rack is waiting on PDU hardware.
- Active Infrastructure Issues
  - None

Open CI Updates - Current Priorities

Top Priorities - End of FY22

- Integrate MISRA into TF-A
- Complete MbedTLS CI
- Complete Code Coverage
- Complete PSA compliance tests
- Close out outstanding Open CI gaps

Priorities - Next month

- Add ST STM32MP15 Platform to OpenCI Lab
- Finish Code Coverage work
- Wrap up PSA compliance tests
- Complete MISRA M1 infrastructure milestone
- MBed TLS stabilization - monitoring & Maintenance

General Topics

LTS Discussion

- Kicked off on TF-A mailing list
- Discussed in TF-M Tech Forum: no big push beyond the existing Hotfix releases
- Scheduled for TF-A Tech forum **July 14th**
  - Discussion driven by Google & NVIDIA
  - Focus on defining the technical requirements first
  - Once those are clear, effort required and funding conversation will follow
  - Different funding models possible
    a. Centrally funded by the TF.org project fees (by employing an LTS maintainer)
    b. Pool of LTS maintainers from ecosystem/members (round-robin or not)
    c. Other models for spreading the cost more across the community?
  - Boards in OpenCI by project members will benefit from regular LTS testing/validation

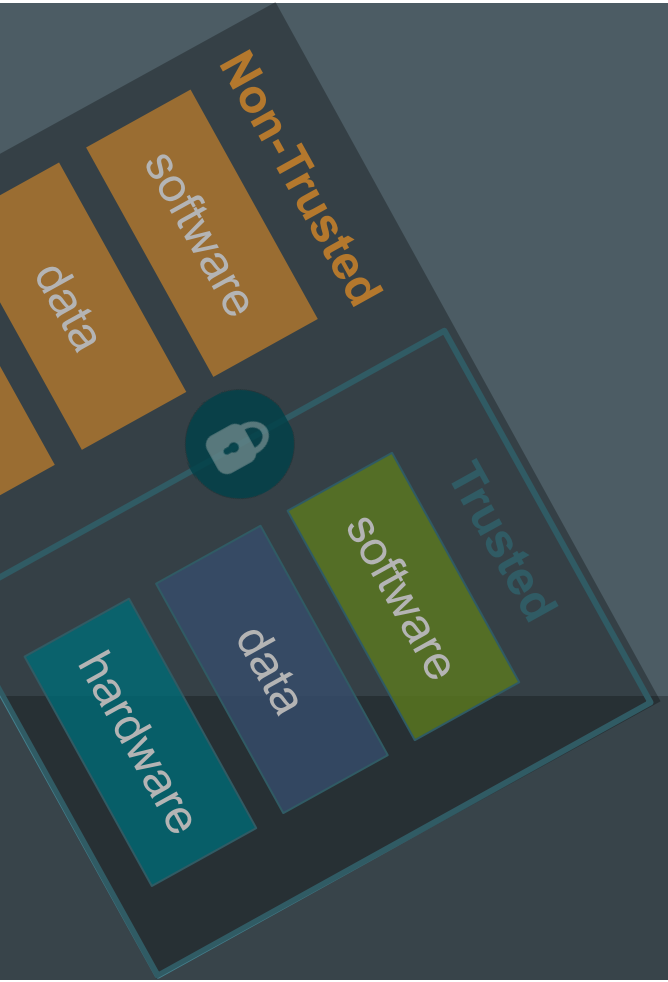
FW Handoff

- Started as a 2021 conversation on standardizing information passing between boot stage
    - https://lists.trustedfirmware.org/archives/list/tf-a@lists.trustedfirmware.org/message/3S3GVT5RLIP2P4YCHC3MR4X2JKQXDE7I/
- Turned into a draft specification on data structures to be used for Firmware Handoff (https://developer.arm.com/documentation/den0135/a)
- Initially proposed by Arm, now traction for an open collaboration on spec development and finalization
- Proposal to host the spec (as a sphinx source format) initially under a repo in Trusted Firmware.org
    - Even though at least Simon Glass (Google/U-Boot) would like to eventually see it as an independent GitHub project

OSFC Sponsorship option

- Open Source Firmware Conference back as an in-person event!
- September 19th - 21st Gothenburg, Sweden
- Open Source Firmware Conference
- Sponsorship increased from last 2 years virtual events (back to in-person prices)
- Any interest in attending and/or sponsoring?

SPONSORSHIP PACKAGE	BRONZE	SILVER	GOLD	CO - ORGANIZER
Complimentary registration	1	2	4	10
Recognition on Twitter	1	3	5	custom
Recognition in newsletter	1	2	2	custom
Keynote logo	✔	✔	✔	✔
Logo & link on event website	✔	✔	✔	✔
Logo displayed in track breaks	✔	✔	✔	✔
Logo placement at the end of video proceedings		✔	✔	✔
Logo placement at the beginning of video proceedings			✔	✔
Promotional items in conference bag			✔	✔
Promote your company for match making via social media / newsletter			✔	✔
Logo on lanyard				✔
Custom branding of the conference				✔
Keynote speaker				✔
Seat in the program committee				✔
	3.000,00€	**6.000,00€**	**10.000,00€**	**30.000,00€**
Exhibit table optional bookable incl. 1 roll-up	add. 3.000,00 €	add. 1.000,00 €	add. 1.000,00 €	included



Open CI TSC Slides - July Preview

Linaro

Status Updates - Boards

In Progress

- TFC-219 Setup New Rack for Cambridge Lava Lab
  - Rack in place, switch ordered, UPS cabling and dispatcher.
  - PDU delayed due to supply chain
- TFC-224 Add ST STM32MP15 Platform to OpenCI
  - Boards in Cambridge; install blocked awaiting new rack

Next

- TFC-100 Add Renesas EK-RA6M4 Platform to Open CI
  - Awaiting boards to ship, software upstreamed

Reminders: Current deployed devices, Job test results, EPIC: Trusted Firmware Community Board Enablement

Status Updates

- TFC-4 Enable Mbed TLS in Open CI
  - Monitoring for stability, performance and cost
- TFC-1 PSA Compliance Tests
  - TFC-57 PSA Compliance Tests - FirmwareFramework resolving test failures
- TFC-7 Code Coverage Tool
  - TFC-268 TF-M CC Tool: Skip check in “platform dir”
  - TFC-281 TF-M CC Tool: “Connection Closed” error - debugging
- TFC-10 Enable MISRA Testing
  - See next slide
- **Next**
  - Finish Code Coverage work
  - Wrap up PSA Compliance Tests
  - Complete MISRA tooling planning
  - TF-A Feature - Repositories sync based on Gerrit topics

MISRA Tooling Update

- Activities in progress for MISRA enablement
  - Beginning with TF-A
  - Epic: TFC-10 in the process of being updated
  - Project in progress with M1: Infrastructure

Plans:

- Complete Infrastructure setup - Licensing and Docker issues

Resolved Tickets - May

- To track/review, click on the Jira filter here

T	Key	Summary	Assignee	Reporter	P	Status	Resolution
	TFC-272	PSA Compliance Tests - FirmwareFramework	Paul Sokolovskyy	Paul Sokolovskyy		RESOLVED	Done
	TFC-294	Grant permission to Satish	Maria Högberg	Xinyu Zhang		RESOLVED	Delivered
	TFC-277	TFC-272 / PSA FF testsuite has 6 failures	Xinyu Zhang	Paul Sokolovskyy		RESOLVED	Done
	TFC-293	Flash on stm32l562e-dk-02 needs to be checked	Dave Pigott	Xinyu Zhang		RESOLVED	Done
	TFC-291	Gerrit Query Limit for TF-A Tests project	Kelley Spoon	Joanna Farley		RESOLVED	Delivered
	TFC-282	OpenCI TF-A Production Code Coverage broke with gen_merge_report patch	Paul Sokolovskyy	Joanna Farley		RESOLVED	Done
	TFC-269	OpenCI TF-A False positive Jenkins Test result (Bug)	Arthur She	Joanna Farley		RESOLVED	Delivered
	TFC-265	TFC-7 / TF-A: Make collective codecov report have source links	Paul Sokolovskyy	Paul Sokolovskyy		RESOLVED	Done
	TFC-279	SQUAD metrics Issues in Production - stopped working	Arthur She	Glen Valante		RESOLVED	Delivered