Linaro Connect
MADRID 2024 | MAY 14-17 2024

SystemReady as the default option for BSPs

Findings from the Feb’24 SystemArchAC workshop - Security and interoperability for Rich IoT devices

SystemReady as the default option for BSPs

Security and interoperability for Rich IoT devices workshop

What is SystemArhAC? Where SystemReady IR is curated

Who can join? Any one with a generic NDA in place

What's been discussed? SystemReady's direction of travel, priorities and specs*

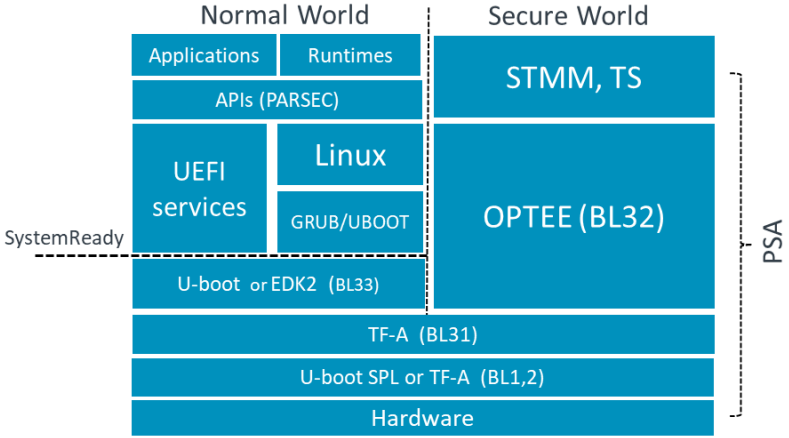
F2F Workshop: 8th and 9th February'24 in Cambridge, UK

Intent: Agree on a common view of what a good reference implementation for a secure and interoperable Rich IoT device would be.

Participants: Arm SR, PSA & PARSEC, Linaro, RedHat, Canonical, LVFS, ST, Eurotech, 56K.cloud, Foundries.io

Agenda, conclusions and challenge ahead – BoF

SW stack diagram



- Governing principles driving design choices around:
  - Boot
  - Maintenance
  - Security
- Standards supporting those principles
- Existing technologies supporting design choices and standards

Outcomes and conclusions:

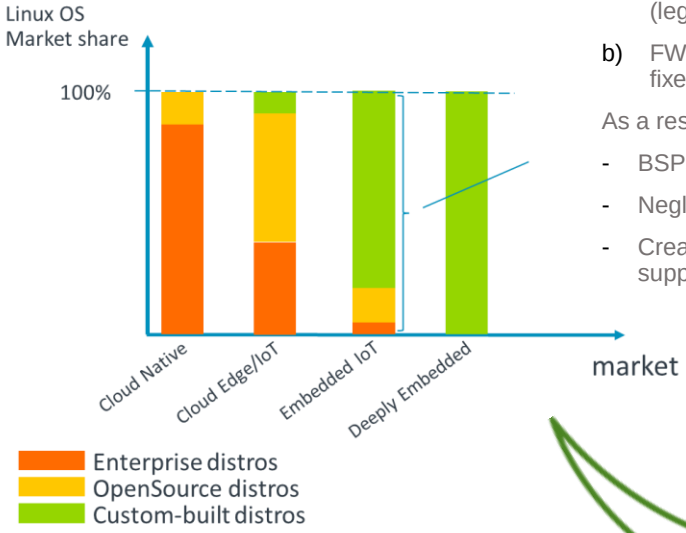
Not many gaps to be fulfilled to achieve a good ref-stack

- Boot level gaps
  - Chain of trust issues when mixing u-boot and TF
  - HTTP/HTTS boot issues related to exitboot service and installation
- Maintenance
  - SMBIOS
  - LVFS and A/B support
- Security
  - Security is achieved through PSA
  - Interoperability for security is achieved through SystemReady

The reasonable question then is:

- Given there’re not so many gaps to be fulfil what is so hard for vendors to make SystemReady the default option for their BSPs
- What is the path of less resistance to make vendors considering SystemReady as their default option?

Supporting slides



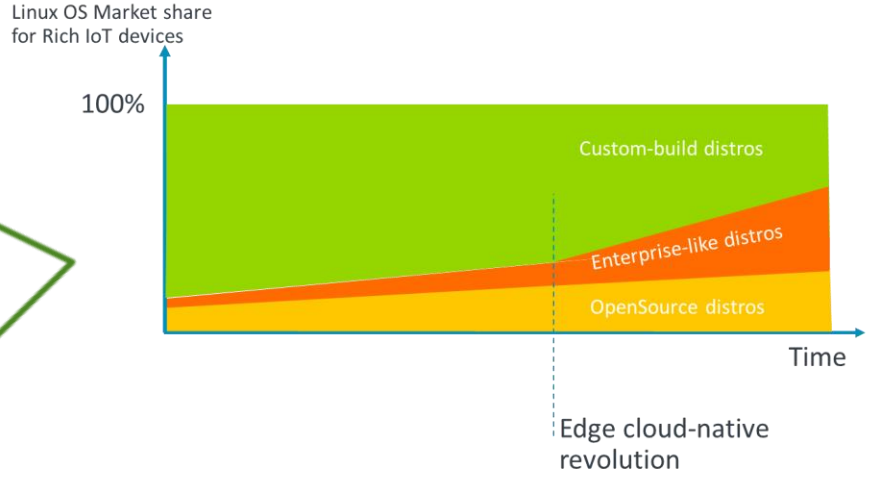
Vendors currently joggling with different FW codebases:

a) FW supporting custom builds OSes - which is not SR compliant by design restrictions (legacy support & other sunk costs)

b) FW supporting pre-build distros – typically a one-off branch from the previous one, with fixes to make it SR compliant

As a result, vendors focus on non-SR firmware paths, prioritizing:

- BSPs with default configurations that lack SR support
- Neglected or unmaintained SR support within BSPs
- Creation of FW for cert purposes, apart from BSPs which is never maintained or supported



Linaro Connect
MADRID 2024 | MAY 12-17 2024

Thank you