ENDIAN TECHNOLOGIES

Meaningful connection.

The ultimate guide to software updates on embedded Linux devices

foss-north 2018

Mirza Krak

endian.se

Session Overview

- Intro
- Basics
- FOSS ecosystem
  - Strategy
  - Key Features
  - Community

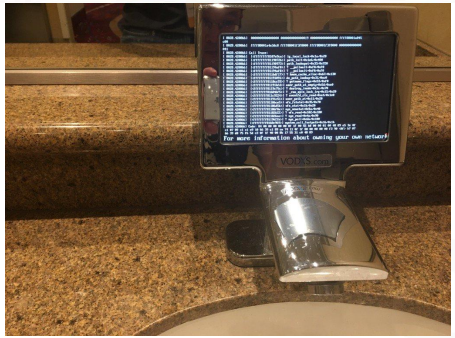
Mirza Krak

ENDIAN TECHNOLOGIES

- FOSS enthusiast
- Board Support Package development
- Linux kernel developer
- Yocto/OE-core
- Disclaimer: Mender community member

Embedded Linux Devices

@internetofshit



Embedded Linux environment

ENDIAN TECHNOLOGIES

- Remote in some cases
  - No physical access to devices
- Long life span
  - 5-10 years
- Unreliable power supply
  - Power loss at any given time
- Unreliable network
  - Mobile
  - Low bandwidth

Why do we need update software?

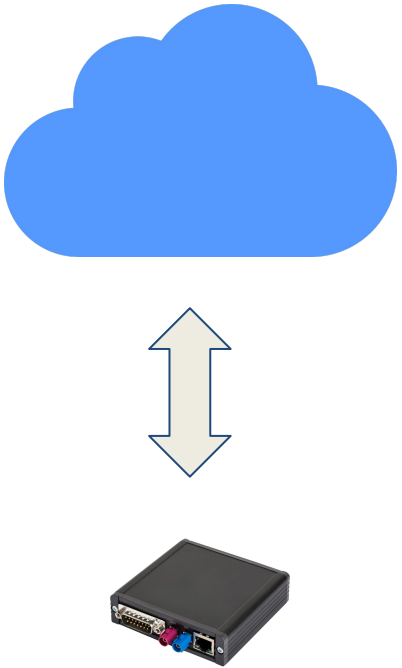
- Fixing issues (bugs)
- Feature growth
- Security updates

CVE-ID	
CVE-2013-4434	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
Dropbear SSH Server before 2013.59 generates error messages for a failed logon attempt with different time delays depending on whether the user account exists, which allows remote attackers to discover valid usernames.	

Software update on-site

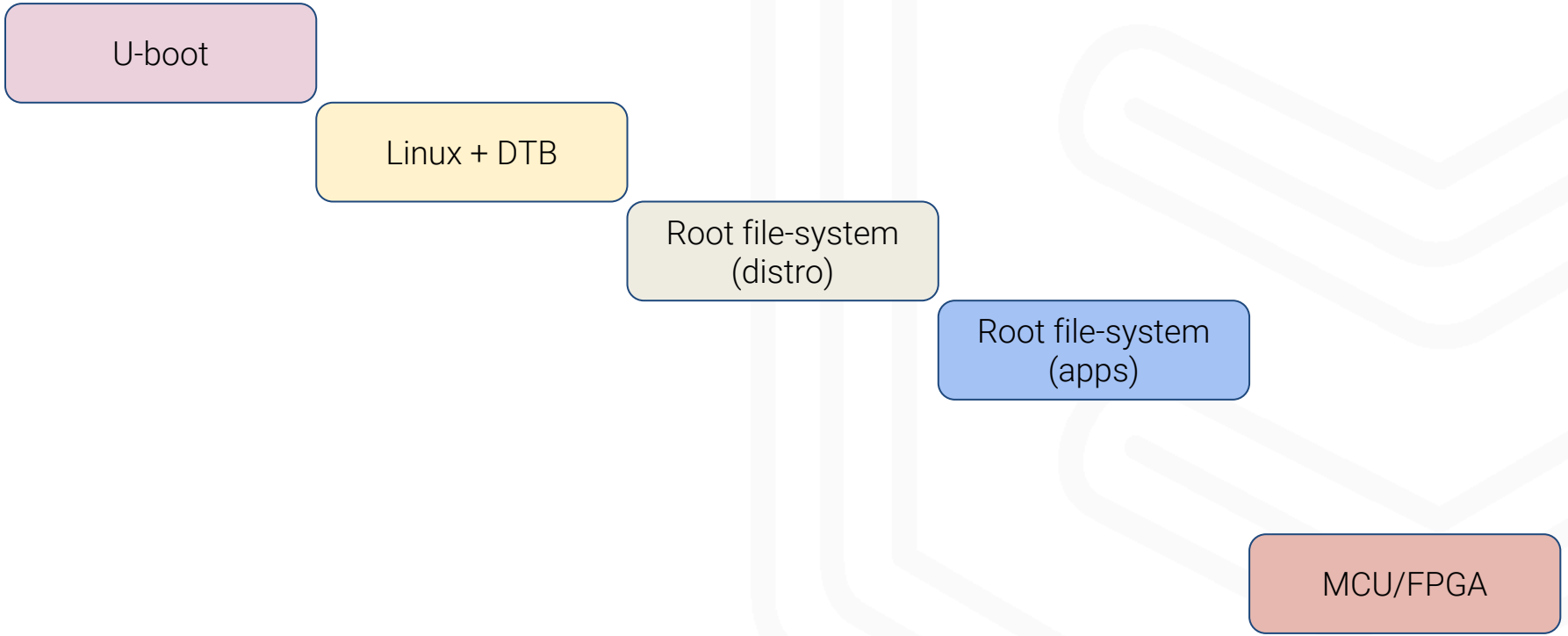
- No connectivity
- Easy access to an device
- USB Flash drive
- Technician

Software updates (OTA)



- No easy access to device
- Deployment management server
  - status reports
  - current versions

What to we need to update?

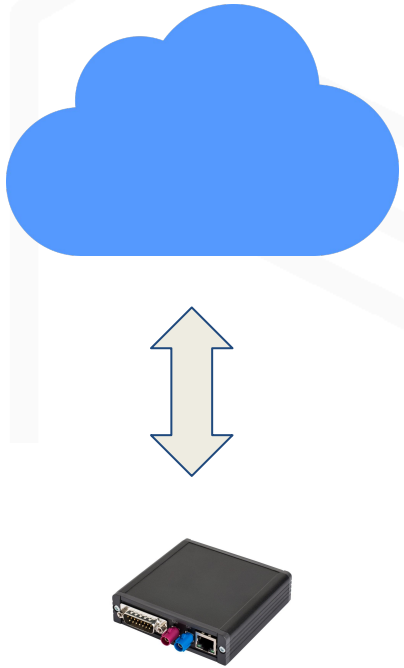


Requirements (basic)

- Able to update all components
  - Unsafe to update bootloader
- Never render the device unusable (brick)
  - Fail-safe
- Atomic updates
  - No partial install
- Roll-back
  - Not always possible
- Integrity check
- Signed images
  - Trusted images
- Compatibility check
- Persistent data storage

Requirements (basic OTA)

- Secure communication channel
  - Encrypted
- Device Authentication (trust)

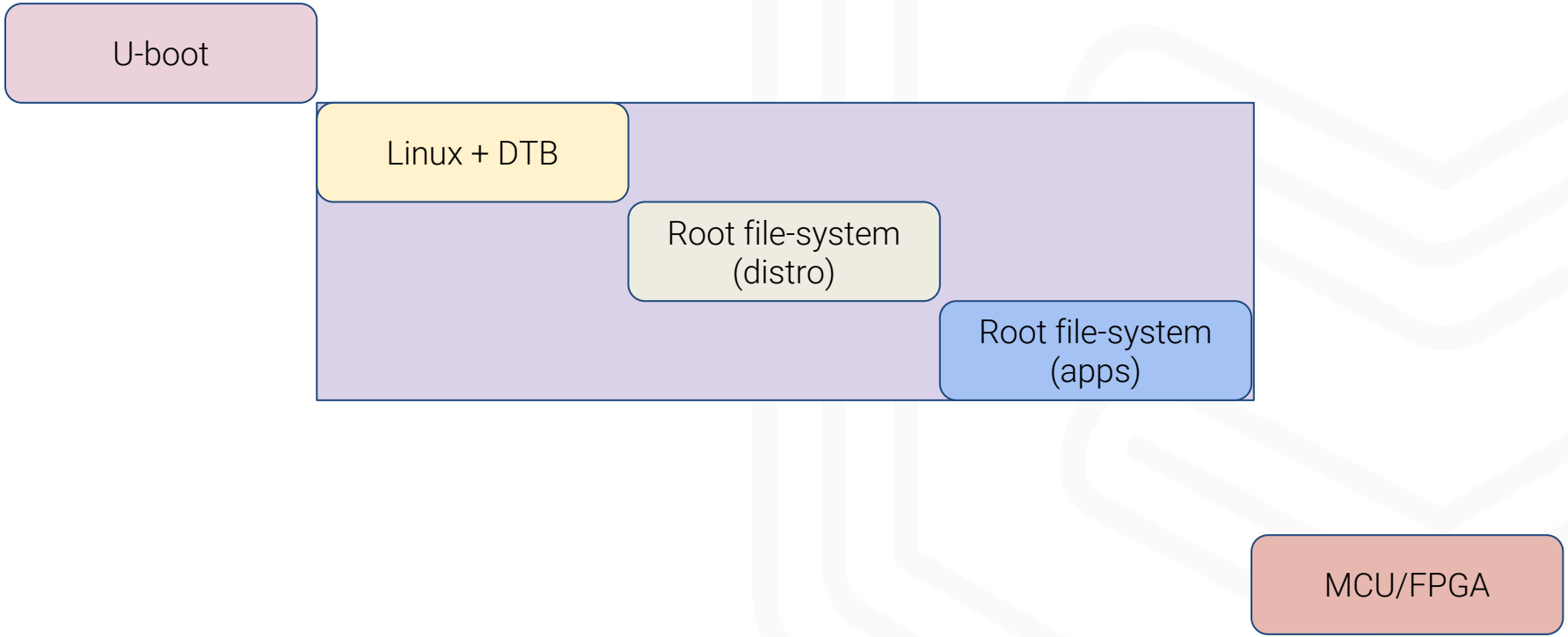


Alternative approaches

ENDIAN TECHNOLOGIES

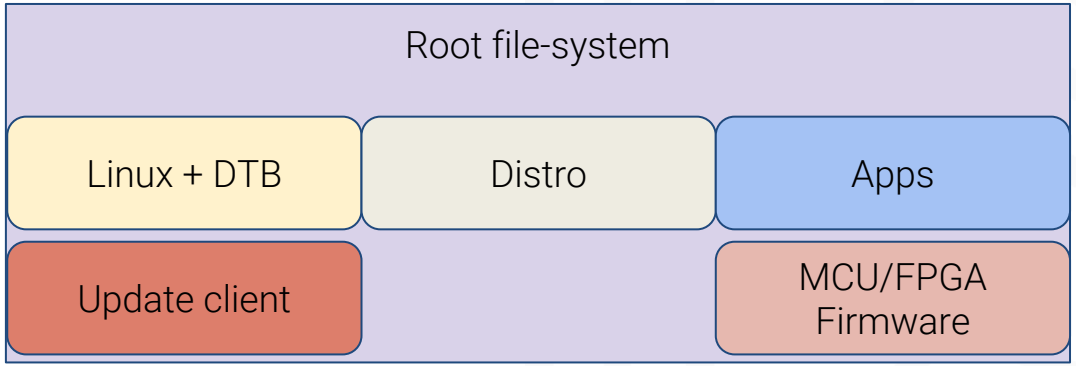
- Image/block based updates
  - Easy to implement, test, verify and maintain
- Incremental atomic image upgrade mechanism
  - Complexity
- Containers
  - Run applications in containers on device
- Package managers (dpkg, dnf, opkg)
  - Not designed for embedded use-case
  - Not atomic
  - Hard to maintain

Image

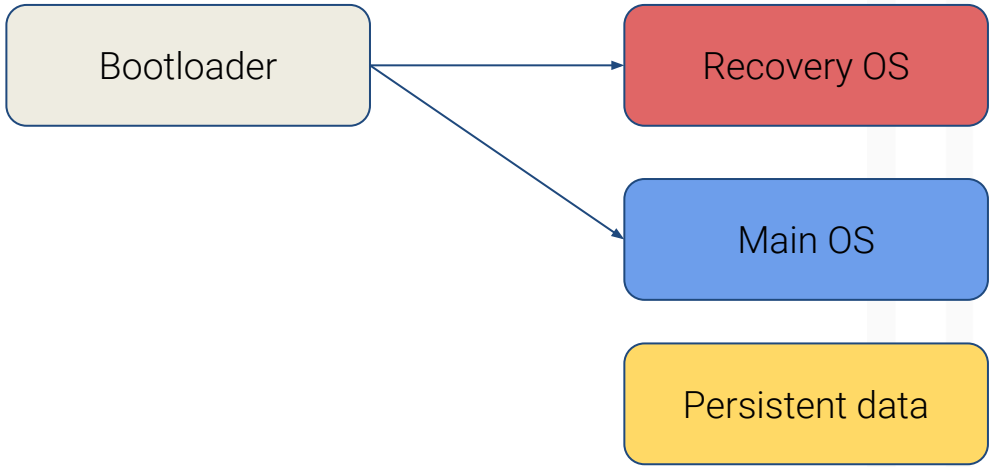

U-boot
Linux + DTB
Root file-system
(distro)
Root file-system
(apps)
MCU/FPGA

Image

/

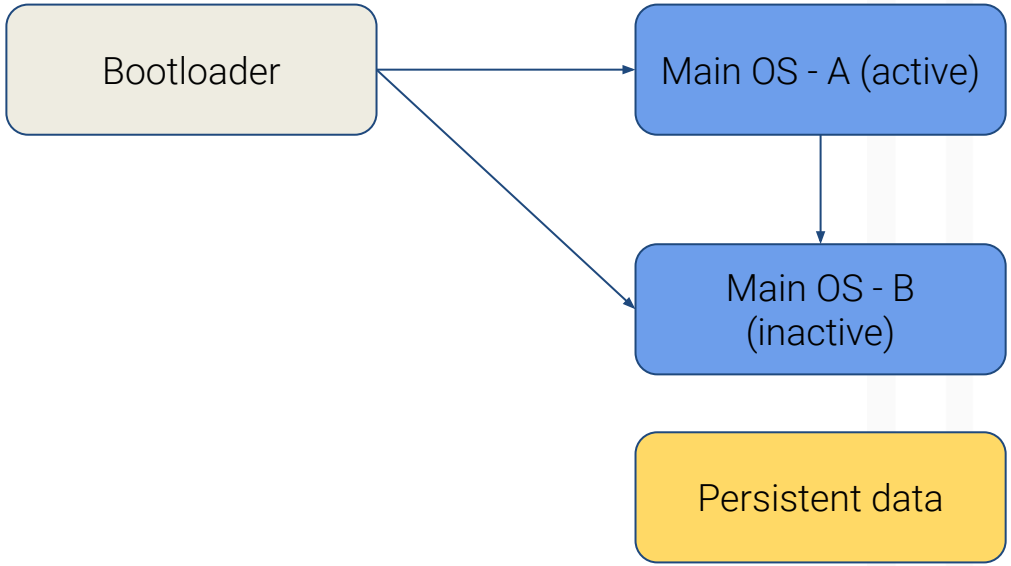

Root file-system
Linux + DTB
Distro
Apps
Update client
MCU/FPGA
Firmware

Asymmetric Image updates



- Think Android (pre N)
- Fail-safe
- Downsides
  - Downtime
  - Intermediate storage

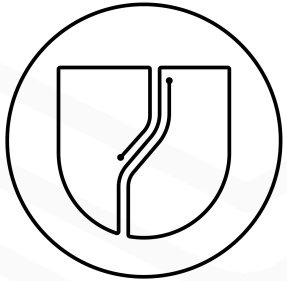
Symmetric Image updates



- Android (post N)
- Seamless updates
- Fail-safe
- Roll-back
- Downsides
  - Double copy of OS

FOSS ecosystem

ENDIAN TECHNOLOGIES

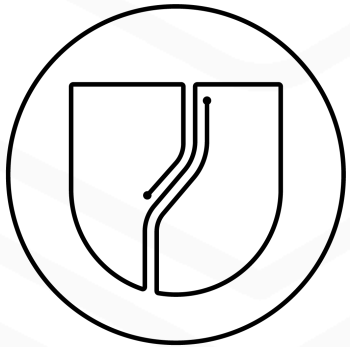


Frameworks

SWUpdate

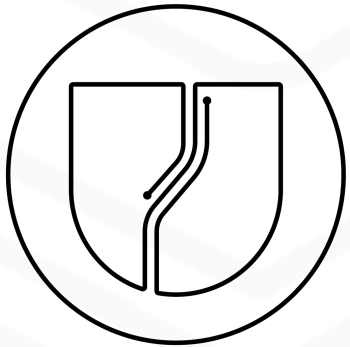
"SWUpdate is a Linux Update agent with the goal to provide an efficient and safe way to update an embedded system"

- http://sbabic.github.io/swupdate/
- C & GPLv2
- Update agent on device
- Tooling to create update images (cpio archives)
- Integrated web server for "local updates"
- Symmetric/Asymmetric Image Updates
- Cryptographic signing and verification of updates



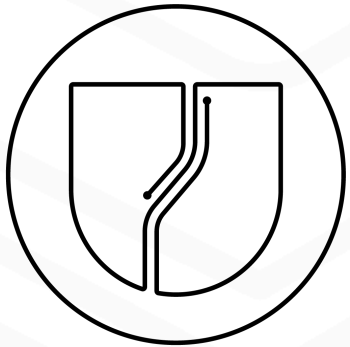
SWUpdate

- NOR / NAND, UBI volumes, SD / eMMC
- UNIX socket interface (status)
- U-boot, grub, EFI
- Yocto
  - meta-swupdate
  - meta-swupdate-boards
- Buildroot
- Integrated support for hawkBit for OTA updates



SWUpdate

- Community
  - 18 releases (4 month cycle, 2018.03)
  - 43 contributors
  - swupdate@googlegroups.com (contributions & issues)
  - Reference boards (BBB, RPi3, Wandboard)



RAUC

"The aim of RAUC is to provide a well-tested, solid and generic base for the different custom requirements and restrictions an update concept for a specific platform must deal with"

- https://rauc.readthedocs.io/
- C & License LGPLv2.1
- Update agent & host tooling
- Symmetric/Asymmetric Image Updates
- Integrate well with application
- Delta updates (casync)
  - experimental

RAUC

- D-Bus interface
- SD/eMMC, UBI, raw NAND
- U-boot, grub, barefox, EFI
- Yocto (meta-rauc) and PTXdist support
- hawkBit client for OTA updates
  - python library

RAUC

ENDIAN TECHNOLOGIES

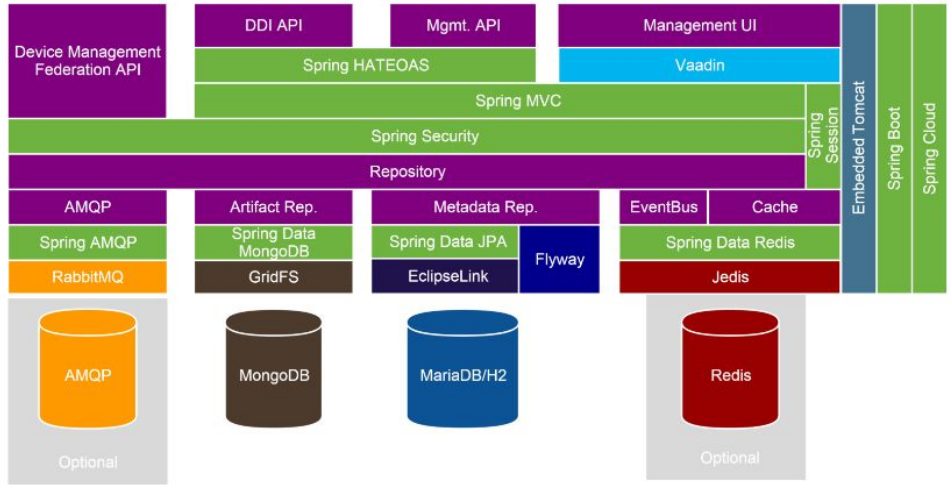
- Solid test infrastructure
  - 70 % code coverage
- Community
  - 6 releases (v0.4)
  - 24 contributors
  - #rauc on freenode
  - Contributions and issues on Github
  - No reference boards?

hawkBit

"Eclipse hawkBit is a domain independent back-end framework for rolling out software updates to constrained edge devices as well as more powerful controllers and gateways connected to IP based networking infrastructure."

- Java & EPL-1.0

Overview of hawkBit modules and used 3rd party technology:



libostree

ENDIAN TECHNOLOGIES

"git for operating system binaries"

- https://ostree.readthedocs.io
- C & LGPLv2
- Image updates
  - Binary deltas
- Complex

libostree

ENDIAN TECHNOLOGIES

- Structure
  - /ostree/repo
  - /ostree/deploy
  - /ostree/deploy/$OSNAME/$CHECKSUM
- /usr is hard links to deploy directory
  - /usr is read-only
- Never boot to physical rootfs
  - initramfs chroot to “deployment”
- Persistent state in /var

libostree

ENDIAN TECHNOLOGIES

- Target platform: PC running Linux.
- Not 100 % on embedded
  - Only ONE file-system (brickable)
  - OStree is part of the ONE filesystem (brickable)
  - No built-in roll-back logic
  - /etc “merge” not suitable for embedded usage
- Yocto integration
  - meta-updater
  - Raspberry Pi 3

libostree

- Gnome Continuous
- Qt OTA
- Flatpak
- Project Atomic
- Aktualizr (GENIVI SOTA)

swupd

- Incremental atomic upgrade mechanism
- https://github.com/clearlinux/swupd-client
- https://github.com/clearlinux/swupd-server
- C & GPLv2
- ClearLinux
- Similar to libostree in functionality
  - No required reboot to apply update
- Yocto
  - meta-swupd (inactive)
- Community
  - Intel only

End-to-End solutions

Mender

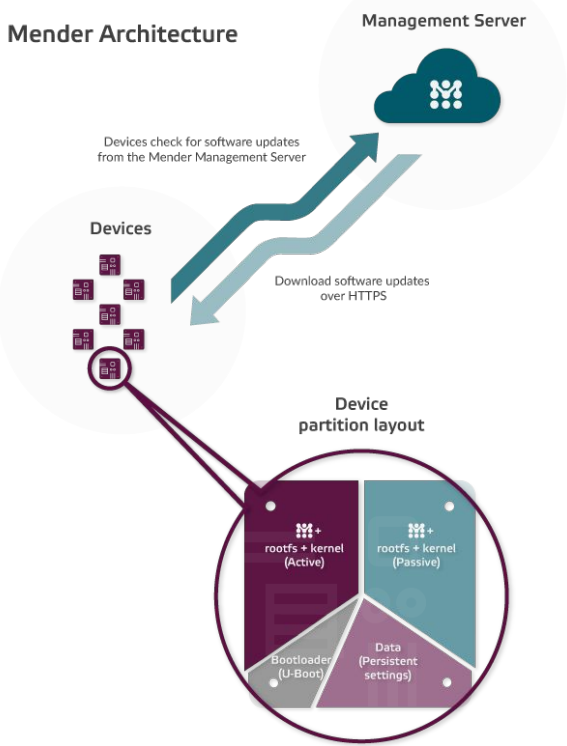
ENDIAN TECHNOLOGIES

"Mender is an end-to-end open source updater for connected devices and IoT"

- https://docs.mender.io/
- Golang & Apache 2.0
- Update agent on device
- Tooling to create update artifacts (mender-artifact)
- Open source management server (backend and frontend)

MENDER

Mender



- Symmetric A/B image update
- TLS communication between client/server
- Streaming of update
- Deployment management
- Device console
- Cryptographic signing and verification of updates

Mender

ENDIAN TECHNOLOGIES

- Yocto integration
  - meta-mender
- 75 % test coverage on client
- QA (open-source)
  - Integration tests on qemu, Beaglebone Black and RPi3
- Community
  - JIRA - https://tracker.mender.io/projects/MEN/
  - 10 releases (1.4.0)
  - mender@lists.mender.io
  - Contributions on github
  - +30 repos in organization

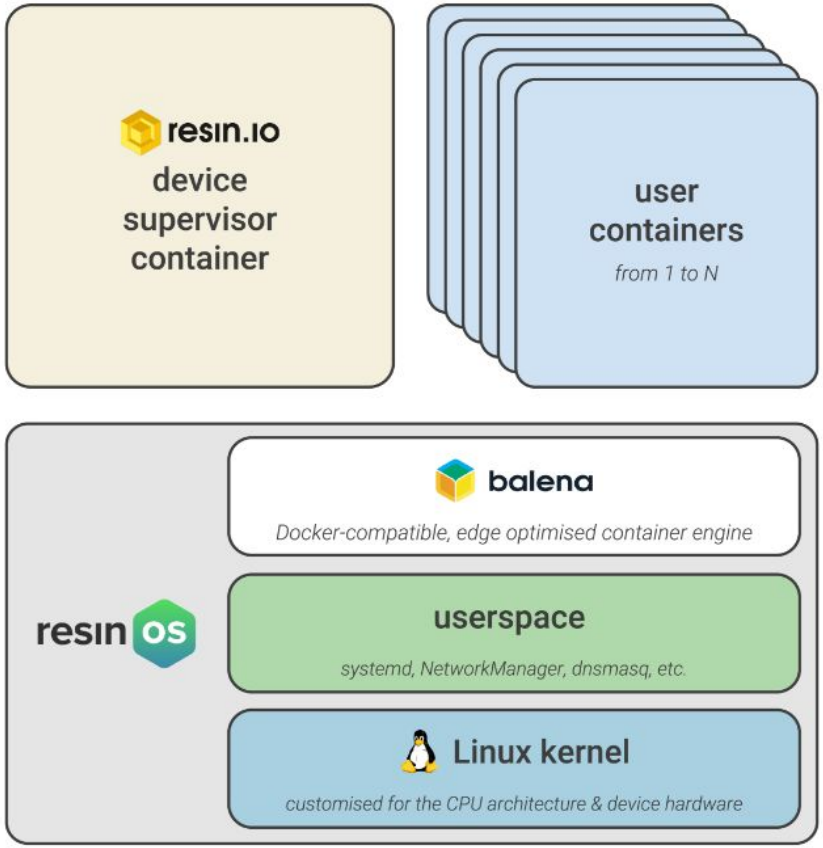
MENDER

resin.io

"Resin.io brings the benefits of Linux containers to the IoT. Develop iteratively, deploy safely, and manage at scale."

- https://docs.resin.io/introduction/
- Proprietary "console" / server
  - Plan to open-source it according to blog
- resinOS
  - open-source

resin.io



- resinOS
- Custom container client
  - optimized for embedded Linux devices
  - container delta updates
- Symmetric A/B image (resinOS)
- Only eMMC/SD support

ATS Garage

"ATS Garage is a tool to manage software updates on embedded devices"

- https://github.com/advancedtelematic
- Aktualizr
  - Client, C++, MPL2.0
  - Built on top of libostree
- ATS Garage
  - Device and deployment management
  - proprietary
- OTA Community Edition
  - No stable releases yet
  - MPL2.0

Updatehub

"Updatehub provides a generic and safe Firmware Over-The-Air agent for Embedded and Industrial Linux-based devices."

- https://github.com/updatehub
- Client and Server Backend under GPLv2
  - Golang
  - HTTP API (actions and status)
- Deployment and device management proprietary?
- Fairly new
  - 1.0.0 released in 2017 Dec

Summary

- Proven solutions
- No reason to go “homegrown”!
- Collaboration

Questions?

?

Thank you!

ENDIAN TECHNOLOGIES

Embedded Linux and beyond

https://mkrak.org