Over-The-Air Update : The Crucial Component of IoT Products

Aravinth Panchadcharam

Senior Embedded Systems Engineer | Maker
Next Big Thing AG

Ethereum Camp Berlin 2018

Introduction

Maker & New Media Artist by Passion

Masters in Electrical Engineering (Electronics, Robotics, Wireless Communication Technologies)

15 years of working experience with corporates, startups, research institutions & art festivals

Currently working as a Senior Embedded Systems Engineer at Next Big Thing AG, Berlin

www.aravinth.info

https://github.com/AravinthPanch

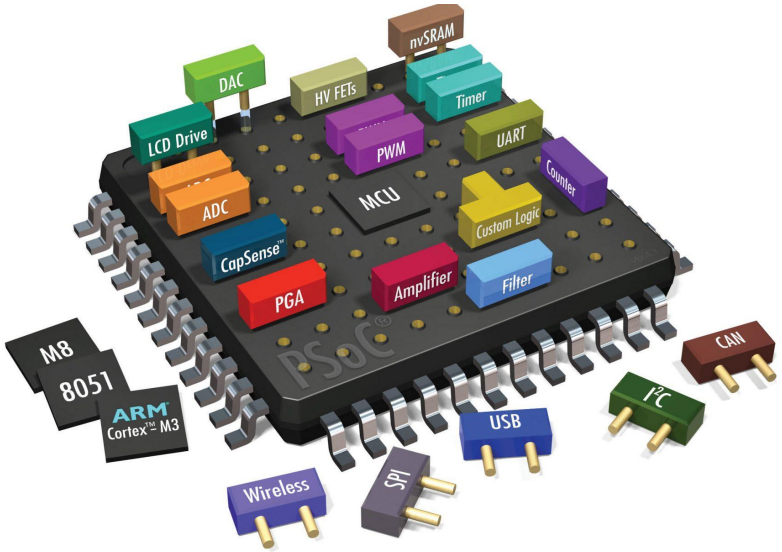
@AravinthPanch

Agenda

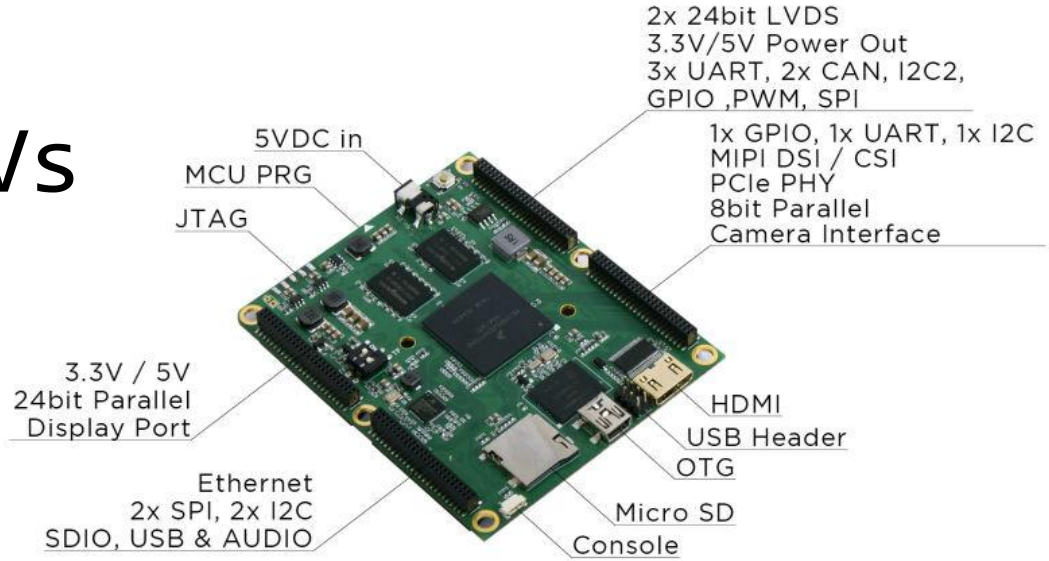
- Rise of Embedded Systems
- Non-Updatable and Bricked IoT Devices
- OTA Update and Rollback Mechanisms
- OTA Update Tools
- Package Management Tools
- Showcase

Rise of Embedded Systems

Functional Specific Vs General Purpose



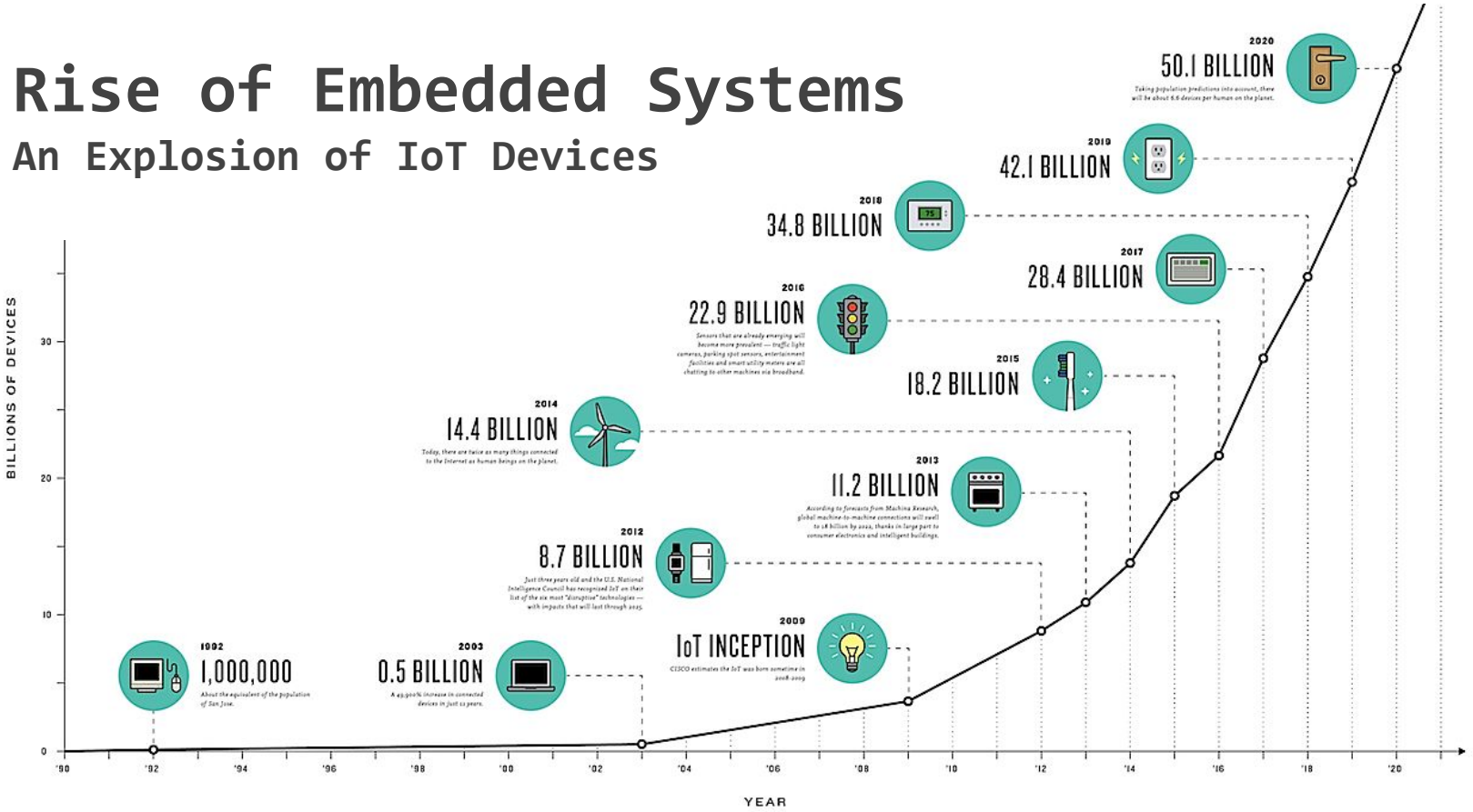
Vs



Source : http://www.cypress.com, https://www.nxp.com

Rise of Embedded Systems

An Explosion of IoT Devices



Source : https://opentechdiary.wordpress.com

Non-Updatable and Bricked IoT Devices

BlueBorne

BlueBorne: Critical Bluetooth Attack Puts Billions of Devices at Risk of Hacking

Tuesday, September 12, 2017 Swati Khandelwal

Share Share Tweet Share Share Mail Share

Source : https://thehackernews.com

Source : https://www.armis.com

Non-Updatable and Bricked IoT Devices

BrickerBot

BrickerBot, the permanent denial-of-service botnet, is back with a vengeance

New botnet squadrons wage fiercer, more intense attacks on unsecured IoT devices.

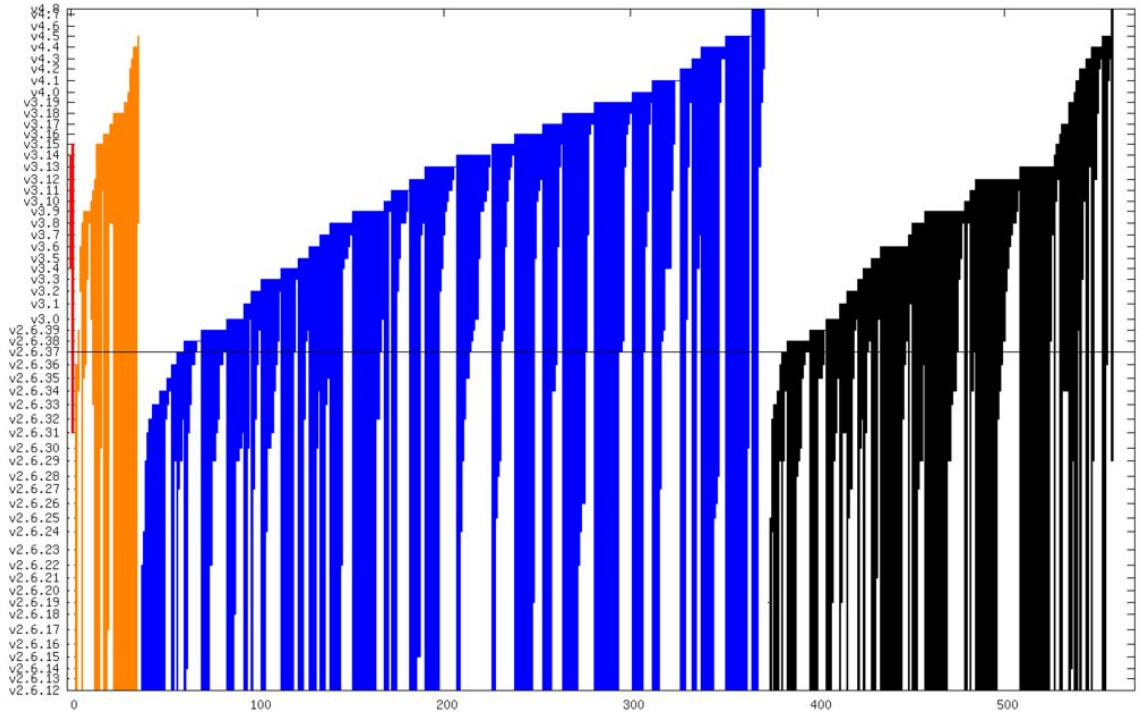
DAN GOODIN - 4/24/2017, 10:43 PM

Source : https://security.radware.com

Source : https://arstechnica.com

Non-Updatable and Bricked IoT Devices

Linux Kernel Bugs and Vulnerabilities



Critical: 3 @ 5.3 years

High: 59 @ 6.4 years

Medium: 534 @ 5.6 years

Low: 273 @ 5.6 years

Source : Kees Cook

Source : https://outflux.net/blog/archives/2016/10/18/security-bug-lifetime

OTA Update and Rollback Mechanisms

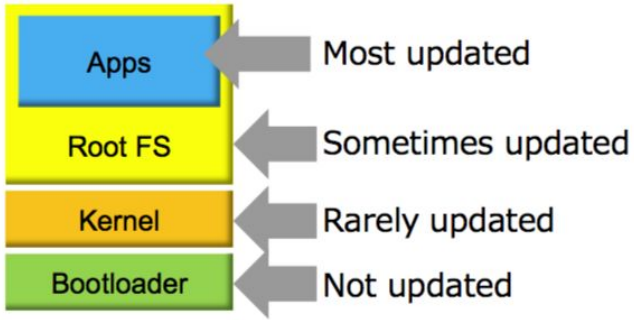
Why do we need an update?

- Security
- Features
- Bugfix
- Migration
- Emergency
- Downgrade

OTA Update and Rollback Mechanisms

Where do we need an update?

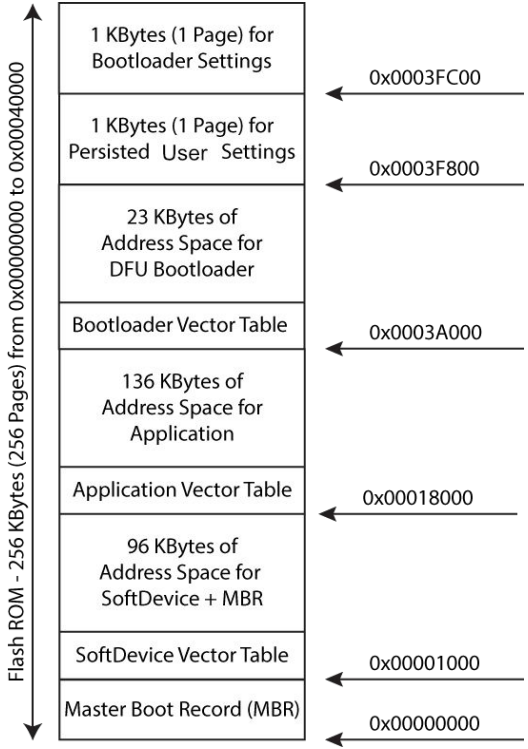
- Bootloader 🔥🔥🔥
- Firmware - Application SoC
- Protocol Stack - Wireless Chipsets
- Kernel + Device Tree - Linux
- System Space - Rootfs
- User Space - Applications
- User Data - Credentials
- Manufacturer Configs - Hardware Constants

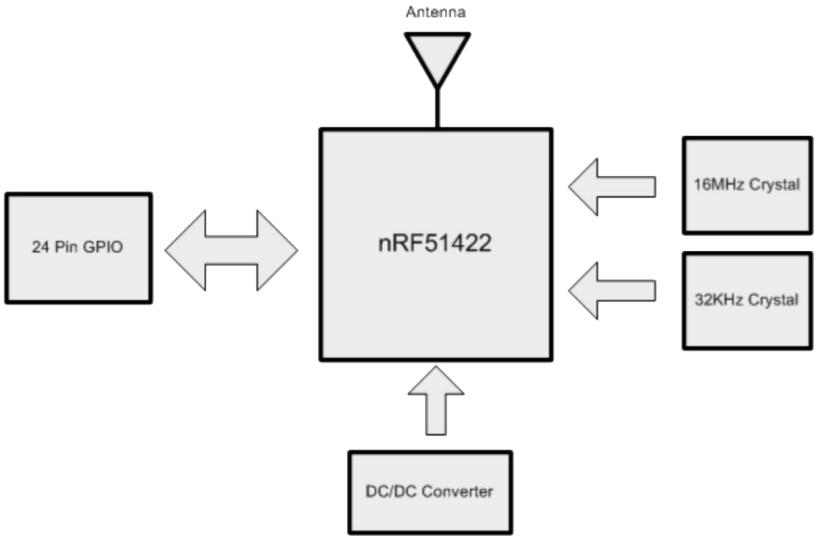


Source : Daniel Sangorrin, Keijiro Yano

OTA Update and Rollback Mechanisms

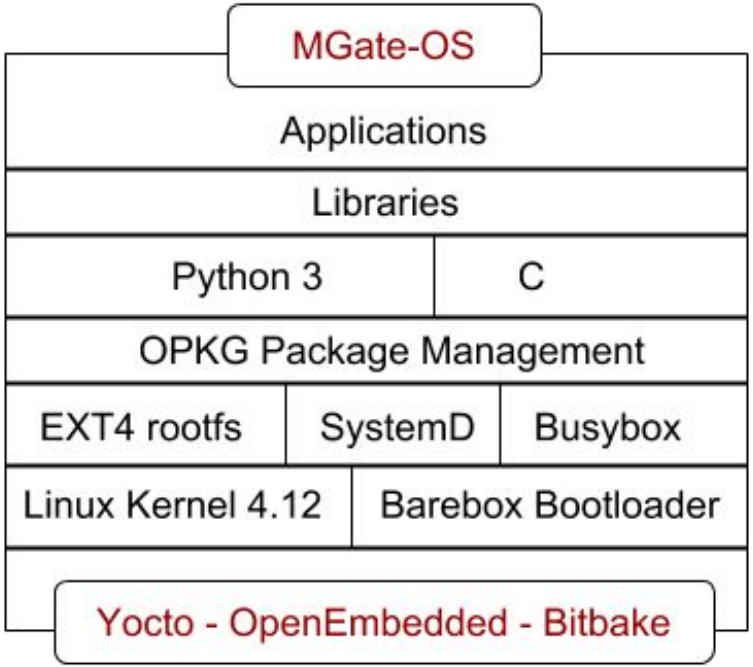
Building Blocks of an IoT Device based on Nordic nRF51 SoC

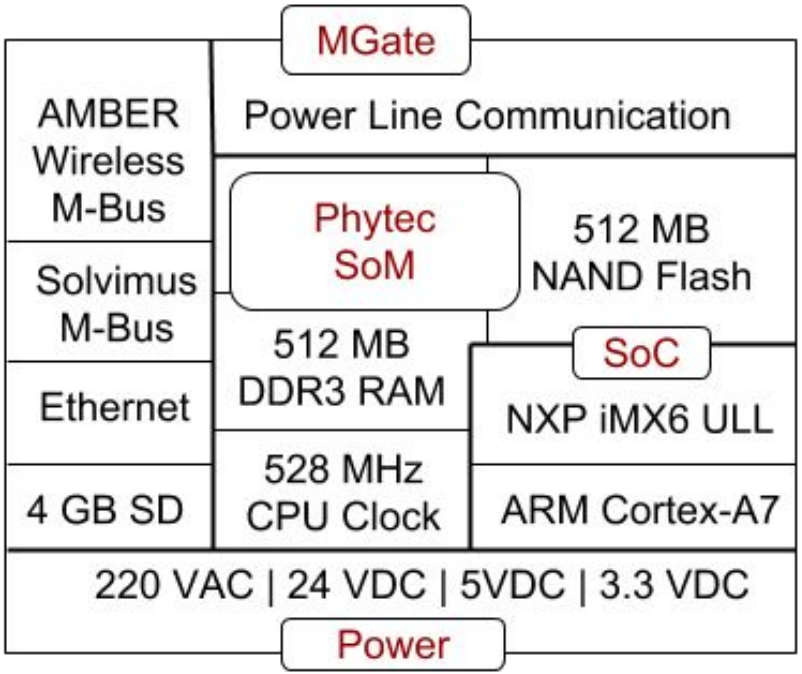




OTA Update and Rollback Mechanisms

Building Blocks of an IoT Gateway based on NXP iMX6 SoC





OTA Update and Rollback Mechanisms

Where is it stored?

- NOR Flash
- NAND Flash
- EEPROM
- eMMC
- SD Card
- USB
- FPGA
- TFTP Server

OTA Update and Rollback Mechanisms

Which interfaces are used to update locally and remotely?

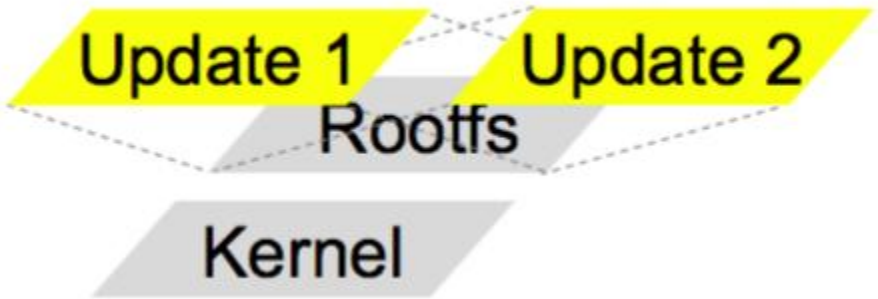
- ISP / ICSP
- SPI
- UART
- USB / CD / LAN - **Manual On-Field Update**
- Bluetooth / WiFi / RF
- GSM / LTE / NB-IoT
- Ethernet / TFTP / Cloud

OTA Update and Rollback Mechanisms

Update patterns

Single Copy Update

- Complete replacement of binary in the memory region
- Common in Microcontrollers, where there is less processing and memory power
- **Nordic nRF-DFU, TI MSP-BSL, arm mBED FOTA**



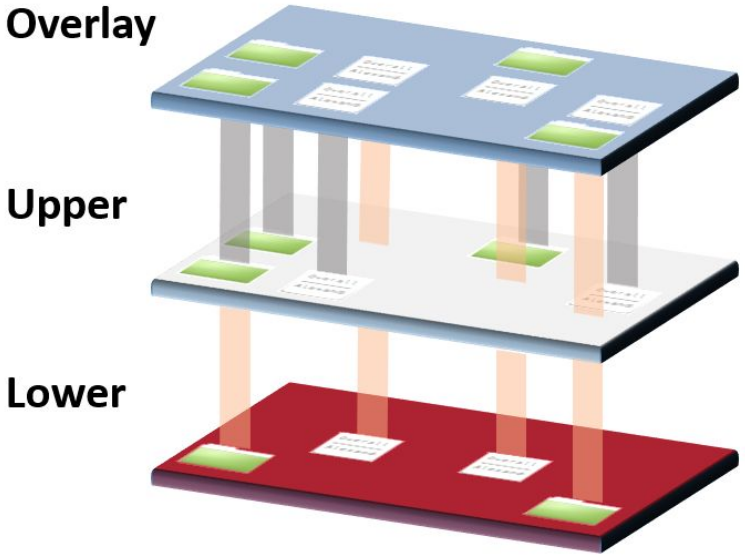
Source : Daniel Sangorrin, Keijiro Yano

OTA Update and Rollback Mechanisms

Update patterns

Overlay or Delta Update

- Replaces parts of the binary in the memory by calculating the delta like in git
- Smaller update package size
- Faster update time
- Higher read and write operations
- **ATS, Ostree, Snappy, HARMAN Smart Delta (used by Tesla), swupdate**



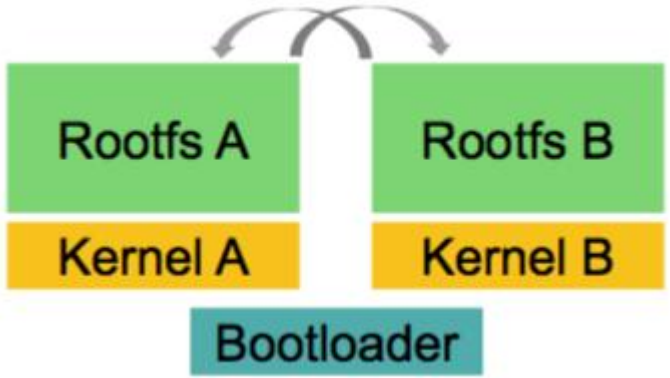
Source : https://www.datalight.com

OTA Update and Rollback Mechanisms

Update patterns

Dual Partition Update

- Atomic update where new image is copied to a swap partition and restarts with new boot partition
- Single image delivery
- Bigger update package size
- Fail-safe and rollback
- Lesser read and write operations
- Automotive grade
- **Mender.io, RAUC, swupdate**



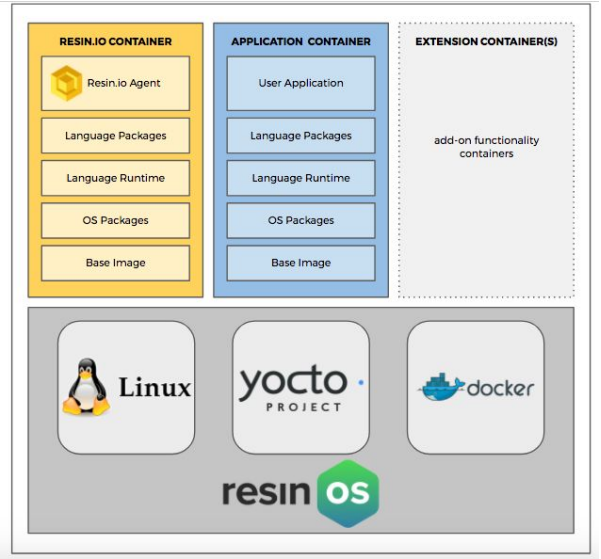
Source : Daniel Sangorrin, Keijiro Yano

OTA Update and Rollback Mechanisms

Update patterns

Containerized Update

- Pull new container image into the userspace like docker
- Low Level Container dependency
- Application development is made easier without worrying underlying hardware
- System space is not updated by default
- **Docker, LXC, Resin.io, Korhal.io, Opendevices.io**



Source : https://resin.io

OTA Update and Rollback Mechanisms

Security, Error Correction, Fail-safe and Rollback

- Signed and verified Update packages
- Secure and verified boot from bootloader to rootfs
- Error correction by checksums, sanity tests and automated tests
- Avoid incompatibilities by updating the complete system with dependencies in an atomic update
- Watchdog enabling to reboot on the stuck update-process
- Rollback to previous version by switching to old boot partition using dual partition update

OTA Update Tools

Mender.io

- Atomic dual partition update & safe rollback
- Web UI for devices, images and deployment management with REST API
- Yocto integration & U-Boot support
- Secure TLS connection between client & server
- 100% open source & Apache License 2.0
- Hosted Enterprise Solution & great support

MENDER.io

Source : https://mender.io

OTA Update Tools

ATS

- Overlay / Delta update based on ostree framework
- Made in Berlin and now acquired by HERE
- Yocto and Buildroot integration
- Open source & Mozilla Public License 2.0
- Automotive grade
- Lightweight update packages

Source : https://www.atsgarage.com

OTA Update Tools

Resin.io

- Containerized Update & Docker/nodejs-based framework
- Image Deltas for fast, lightweight updates
- Support for SBC such as RPi, Beagle, Edison, Toradex iMX6
- Deployment server for device status monitoring, phased deployments and scheduled updates
- Open source & Apache License 2.0

Source : https://resin.io

OTA Update Tools

RAUC

- Most flexible Fail-Safe & Atomic updating tool
- Supports various update modes - dual partition, overlay and etc
- Supports various bootloaders grub, barebox, u-boot, EFI
- 100% open source & GNU Lesser General Public License v2.1
- Hardware watchdog, commandline host, D-Bus API

Source : https://github.com/rauc

Package Management Tools

Higher Level Application Update

- Most of the time complete system update is not needed
- Various tools used for updating higher level applications, which are constantly changing
- Smaller and faster updates & Single Copy or delta updates
- Pre-built packages such IPK, RPM, Deb or builds on the target
- Simple Package Repository Servers

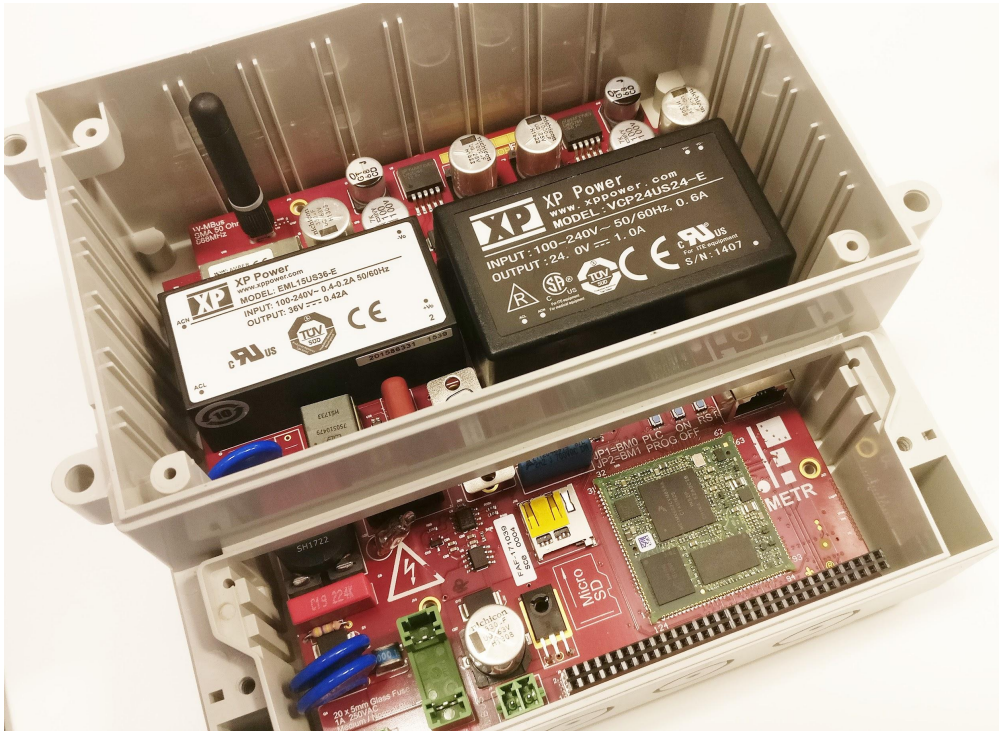
OPKG

PIP

Source : https://wiki.openwrt.org/doc/techref/opkg, https://labix.org/smart, https://pypi.python.org/pypi/pip

Showcase

Updating tools used in my IoT products - NextBigThing AG



M-Gate
M-Bus Sub-Metering Gateway based on NXP iMX6

Mender & OPKG

Source : http://www.nextbigthing.ag

Showcase

Updating tools used in my IoT products - Senic GmbH

Senic HUB
Home Automation Hub based on
Allwinner H3

Mender & Pip
-
Nuimo
Smart Controller based on
Nordic nRF51

Dual Bank Device Firmware Update (DFU) over Bluetooth

Source : https://www.senic.com

Showcase

Updating tools used in my IoT products - smartB GmbH

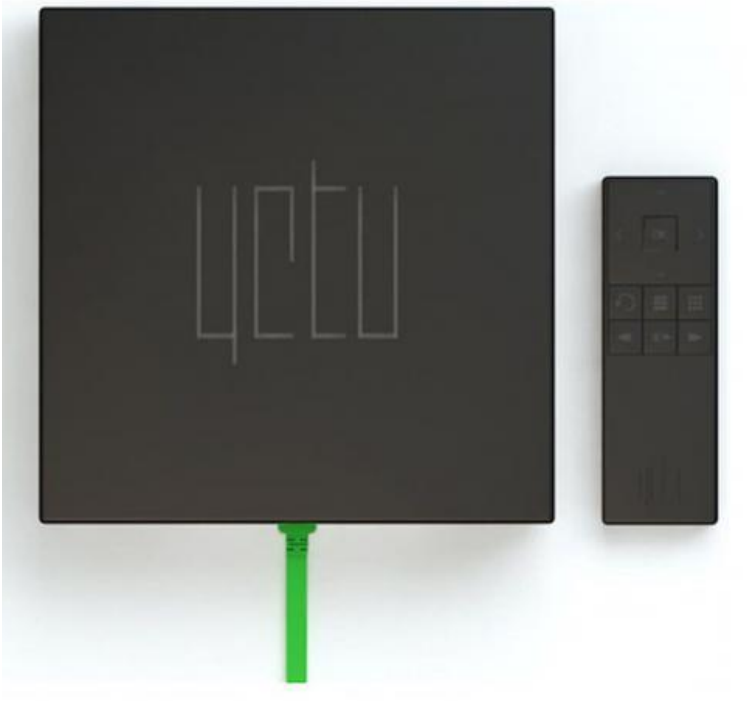
SmartB
Non-Intrusive Load Monitoring Gateway

Home Grown Updater & OPKG

Source : https://www.smartb.de

Showcase

Updating tools used in my IoT products - Yetu AG



Yetu
Smart Home Automation
and Media Center Gateway
based on NXP iMX6

ChromeOS & swupdate

Source : https://github.com/yetu

Thank you

Questions ???