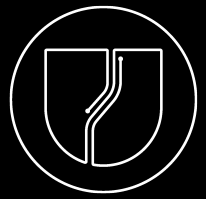
Orchestrated Android-Style System Upgrades for Embedded Linux

Diego Rondini



Update Factory

What this session is about

Manage and rollout software updates

on Embedded Linux devices and apply them

like Android does.

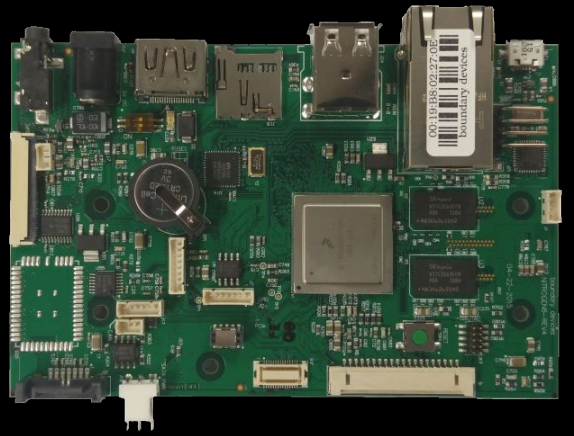
Agenda

- Motivations for our work with OTA updates on Embedded Linux
- The Android way for managing updates
- Embedded Linux updates agent: SWUpdate
- Remote management and rollout campaigns: Eclipse hawkBit
- Our implementation to manage and deploy software updates Android-like: Update Factory
- Demo.

Motivations

- Support medium scale general purpose CPU-SOC modules
- Install atomically a new OS on a device
  - Atomicity of the update
- Track updates and divide them per device types and use cases
- Support custom device metadata sent to the Remote Update Management Platform

Preamble

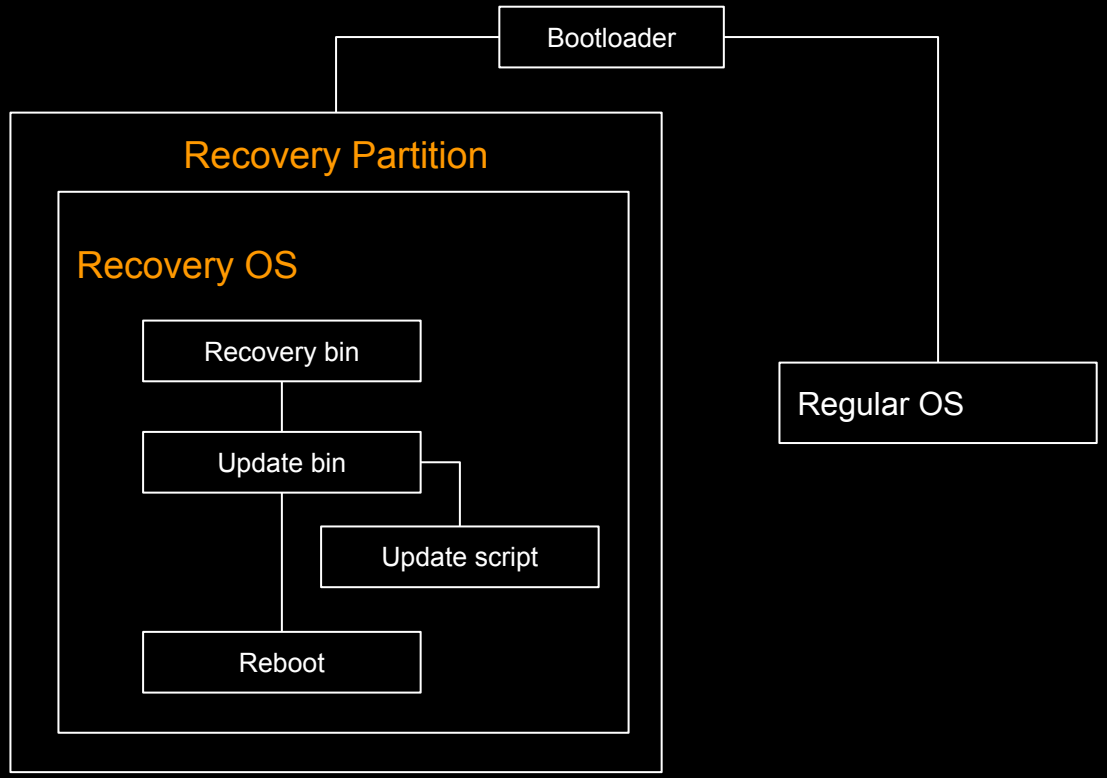


- Boundary Devices Nitrogen6x as reference
  - NXP i.MX6 platform (meta-freescale)
  - U-Boot on NOR flash
  - boot and root partition
- we refer to traditional Android single copy OTA
  - recent Pixel devices with big storage use Chrome OS based double copy OTA
- designed for biggest freedom of storage access while still running in a Linux OS

Android update: approach to OTA updates

- Android approach splits the upgrade process in two phases:
  - preparation for the upgrade → performed in the full fledged Regular OS
  - execution of the upgrade → performed in a purpose built Recovery OS
- Execution performed by the *recovery* binary

Android update Workflow



Android update: preparation

- Preparation on the Device flow:
  - registers to the cloud
  - polls for available updates
  - notifies update is available (Download? Y/n)
  - notifies update is ready to install (Proceed? Y/n)
  - reboot to Recovery OS

- *Verification of package signatures*
  https://developer.android.com/reference/android/os/RecoverySystem.html#verifyPackage(java.io.File,%20android.os.RecoverySystem.ProgressListener,%20java.io.File)
- *Installation setup and reboot in recovery mode*
  https://developer.android.com/reference/android/os/RecoverySystem.html#installPackage(android.content.Context,%20java.io.File)

Android update: execution

- Bootloader/bootscript gets “reset cause” (i.MX6 Family) and boots in ramdisk-based Recovery Mode
- *recovery* starts
- *recovery* unpacks the update file provided (signed zip)
- *update-binary* executes actions in the *updater-script* (edify)
- log and result files are written in the partition
- reboot to Regular OS

- https://source.android.com/devices/tech/ota/device_code
- https://github.com/boundarydevices/android_device_boundary/commit/f069efd28d7d55e1cc298662881b9ceabb4650e3#diff-a55e09ca16b027ed99c01ca6765d9cca

Snippet: bootscript (i.MX6)

```
+setenv bootpart 1
+
+setexpr rval *0x020CC068 \& 0x180        # get reset cause
+if itest.s "x$rval" -eq "x100"; then
+    echo "----------- run fastboot here";
+else
+    if itest.s "x$rval" -eq "x80"; then
+        setenv bootpart 2;
+    fi
+fi
+
+mw.l 0x020cc068 0 1
```

Android Update: advantages

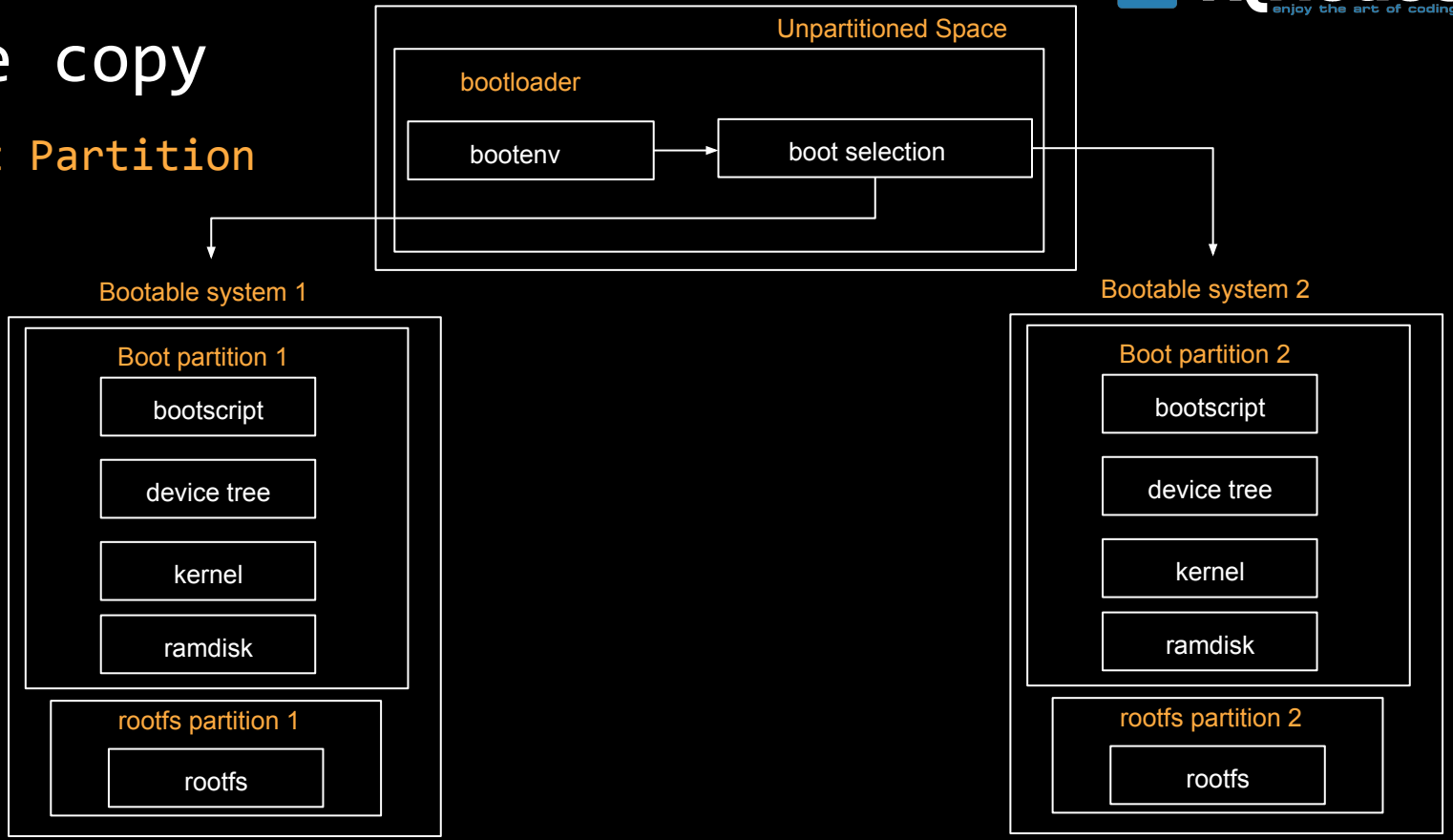
- Single copy update featuring a recovery OS
- OTA agent runs in regular OS
  - No need to interrupt normal operation (yet)
  - Network access (e.g. Wifi setup by the user)
  - Interaction with the user (notifications / acknowledgment)
  - Full API access (Wifi or 3G/4G? Low battery?)
- Recovery has no need of network access, all artifacts are pre-fetched
- Update script support binary writing (no mount is required)
- Recovery environment is RO, minimal, isolated

Part One: Device Update Approaches

- Double copy:
  - The devices features two copies of the Application/OS/RootFS
  - Each copy must contain the kernel, the root file system, and each further component that can be updated
  - Cooperation with the boot loader is necessary to decide which copy should be booted
- Single copy:
  - A separate upgrade OS is required
  - You may update Kernel and Device Tree if the update environment is *segregated*
  - Cooperation with the bootloader is necessary to boot in update mode

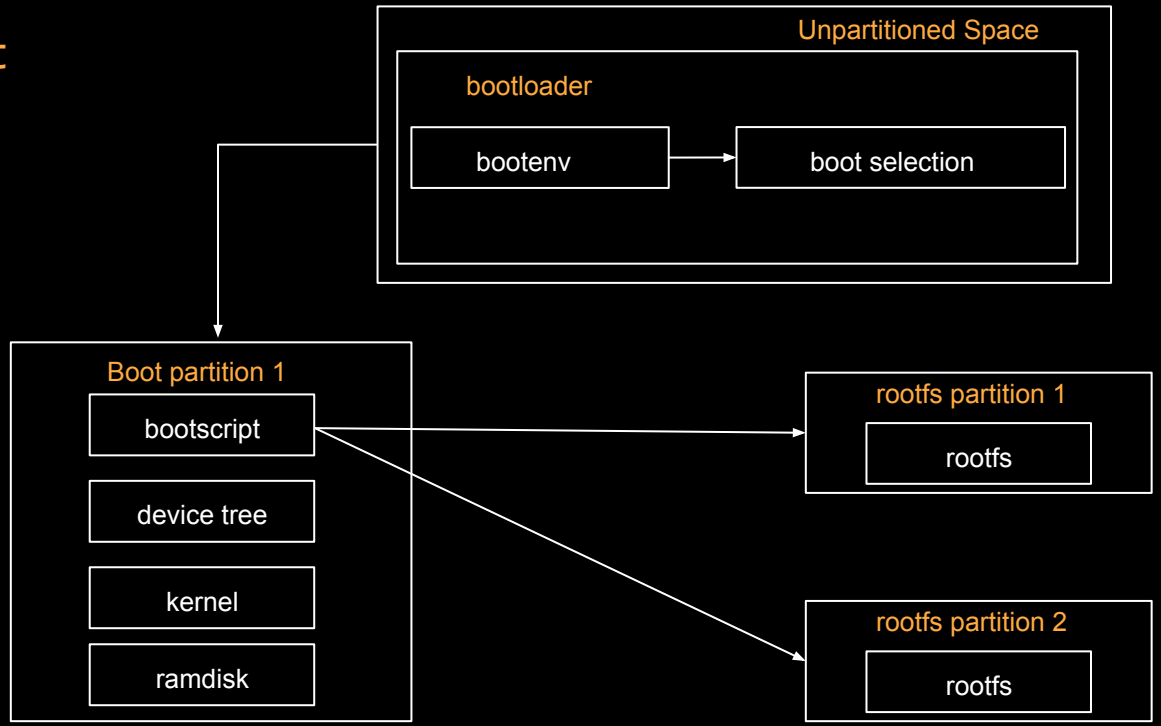
Double copy

Dual Boot Partition



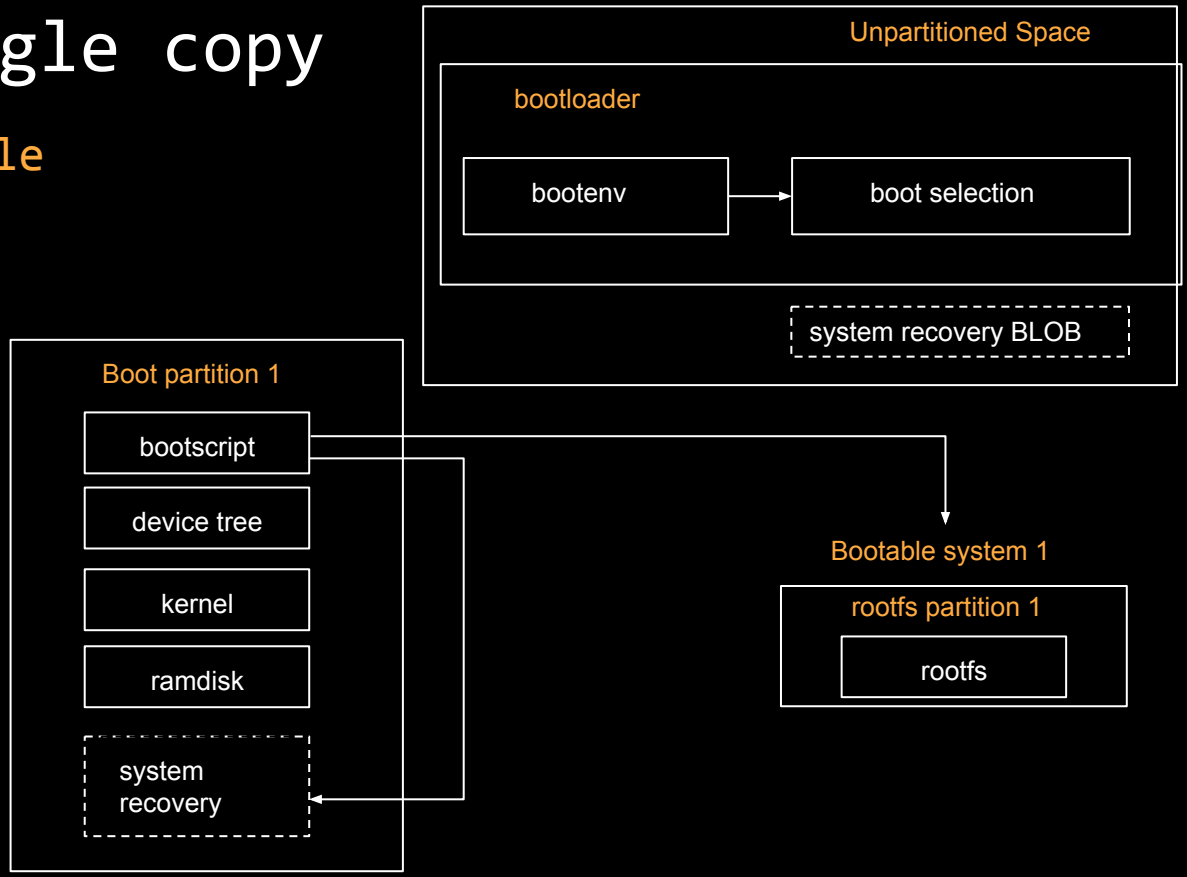
Double copy

Single Boot Partition



Single copy

Simple



Double Copy: Pros and Cons

- Pros:
  - Fallback in case of failure
  - Pretty easy to implement
- Cons:
  - Expensive in terms of storage resources, double the space
  - Requires a mechanism to switch between running and other copy if multiple partitions are doubled (e.g. boot, root)
  - Identify which copy is running

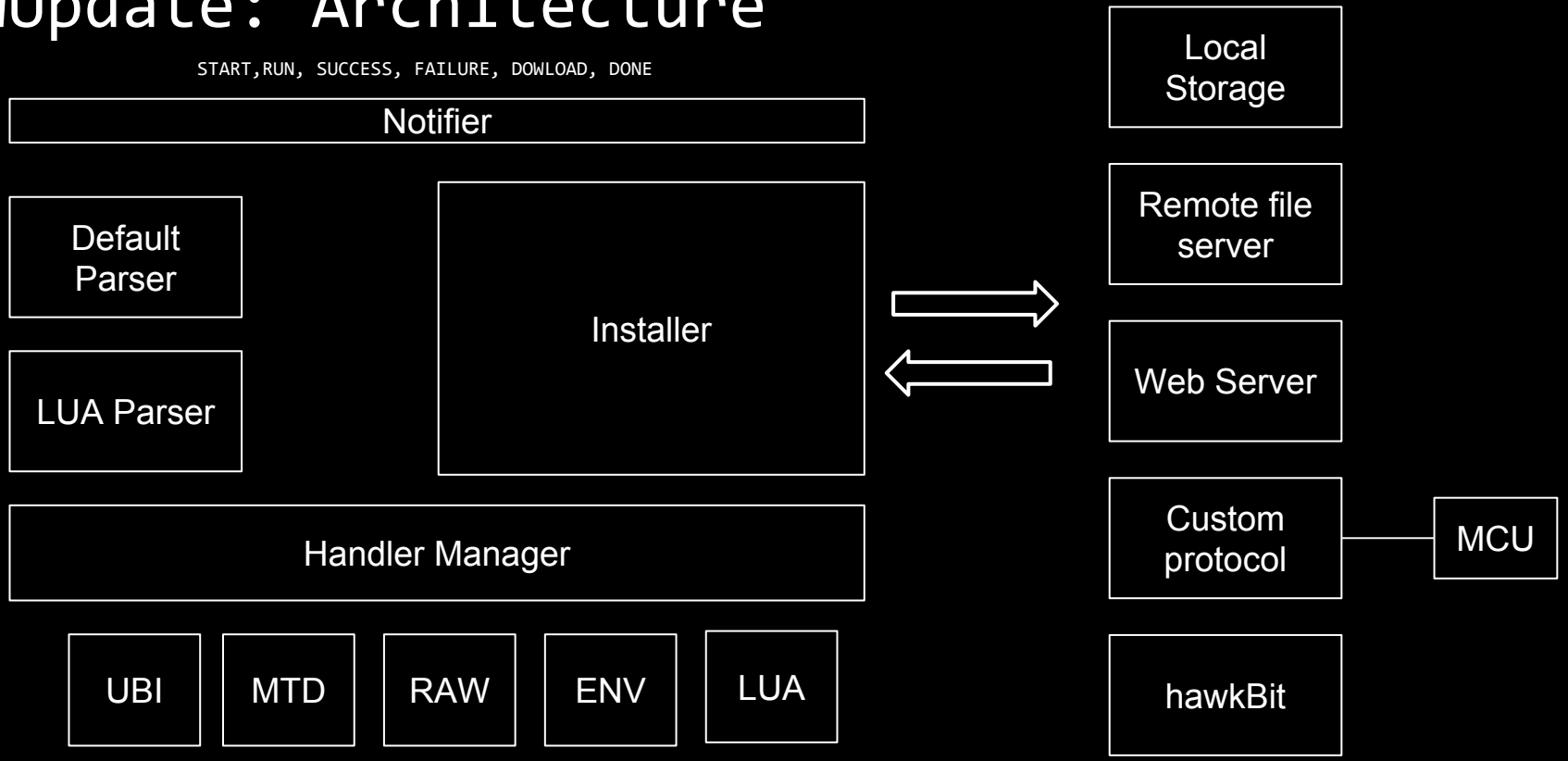
Single Copy: Pros and Cons

- Pros:
  - Requires smaller amount of space
  - “Update mode” lives in RAM
  - Can freely access whole storage (rewrite from scratch, including partition table)
  - Can be used for factory reset (tftpboot / USB boot)
- Cons:
  - No fallback if write fails (e.g. power interruption). Restart recovery mode to try again

Embedded Linux like Android ?

- A good option for building a recovery system “Android Like” Linux is SWUpdate:
  - Written in C by Stefano Babic (Denx) and contributors
  - Runs as Daemon or direct invocation
  - Update files (.swu) based on CPIO format
  - Several handlers (e.g. write raw data, write single file)
  - Update files scripting features (LUA)

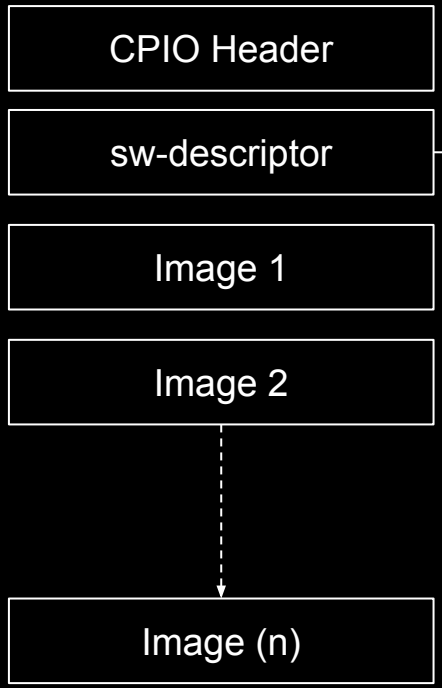
SWUpdate: Architecture



SWUpdate: features

- Local interfaces:
  - Local storage (USB, SD) as artifacts source
  - Support local peripheral devices, through USB/UART for streaming update (i.e MCU)
  - Embedded Web Server as local UI
- Remote interfaces:
  - HTTP, FTP
  - hawkBit (Suricatta embedded client)
- Signature and encryption of update files
- Handlers
  - U-boot for reading environment variables
  - Shell pre/post install scripts (also LUA)
  - Default config parser using libconfig (to parse update description file)

SWUpdate: single image format




```
software =
{
        version = "0.1.0";
        target = {
        hardware-compatibility: [ "1.0"];
        Images: (
                {
                 filename = “rootfs.ext4.”;
                 device = /dev/mmcblk0p2”;
                 type = “raw”;
                 compressed = true;
                }
        );
        scripts:(
                {
                 filename = “installscript.sh”;
                 type = “schellscript”;
                 sha256 = “faaaa30c….”;
                 }
        );
         }
}
```

Security notes

- SWUpdate combines signed sw-description with the verification of hashes for each single image.
  - RSA PKCS#1 (public/private)
  - CMS PKCS#7 (certificates)
- This means that only signed sw-description, generated by a verified source, can be trusted by the installer.
  - sw-description.sig
  - Public.pem can be passed to SWUpdate daemon (on the device)
- sw-description contains hashes for each sub-image to verify that each delivered subimage really belongs to the release.
  - Each image inside sw-description must have the attribute “sha256”

Security notes: sign and configuration

```
#!/bin/bash

MODE="RSA"
PRODUCT_NAME="myproduct"
CONTAINER_VER="1.0"
IMAGES="rootfs kernel"
FILES="sw-description sw-description.sig $IMAGES"

#if you use RSA
if [ x"$MODE" == "xRSA" ]; then
    openssl dgst -sha256 -sign priv.pem sw-description >
sw-description.sig
else
    openssl cms -sign -in  sw-description -out sw-description.sig
-signer mycert.cert.pem \
        -inkey mycert.key.pem -outform DER -nosmimecap -binary
fi
for i in $FILES;do
        echo $i;done | cpio -ov -H crc >
${PRODUCT_NAME}_${CONTAINER_VER}.swu
```

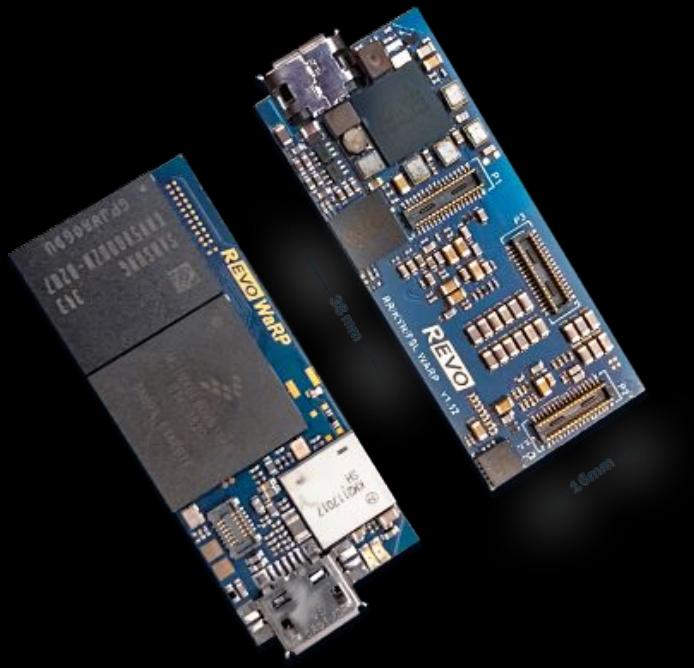
```
software =
{
        version = "0.1.0";

        hardware-compatibility: [ "revC"];

        images: (
                {
                    filename =
"core-image-full-cmdline-beaglebone.ext3";
                    device = "/dev/mmcblk0p2";
                    type = "raw";
                    sha256 =
"43cdedde429d1ee379a7d91e3e7c4b0b9ff952543a91a55bb2221e5c72cb
342b";
                }
        );
        scripts: (
                {
                    filename = "install.sh";
                    type = "shellscript";
                    sha256 =
"f53e0b271af4c2896f56a6adffa79a1ffa3e373c9ac96e00c4cfc577b9be
a5f1";
                 }
        );
}
```

Security notes: encryption

- SWUpdate supports encrypted images
  - SWUpdate allows to symmetrically encrypt update images using the 256 bit AES block cipher in CBC mode
  - encrypted = true parameter in sw-description

```
software =
{
        version = "0.0.1";
        images: ( {
                        filename = "core-image-full-cmdline-beaglebone.ext3.enc";
                        device = "/dev/mmcblk0p3";
                        encrypted = true;
                }
        );
}
```

Case Study: Warp board



- Small wearable reference platform
- Community: www.warpx.io
- Support for SWUpdate for OS updates
- Single image
  - From bootloader, flash stand alone SWUpdate OS Image on the eMMC
    - (UMS): dd img file
    - mmc read ${initrd_addr} 0x2000 0xAA80
  - Boot the SWUpdate OS image
  - Load module for USB over ethernet
  - From a host use browser and upload the SWU image

Part 2: Eclipse hawkBit

The Eclipse Foundation has been very active in promoting significative projects for the IoT, in particular under the umbrella of the Eclipse IoT community.

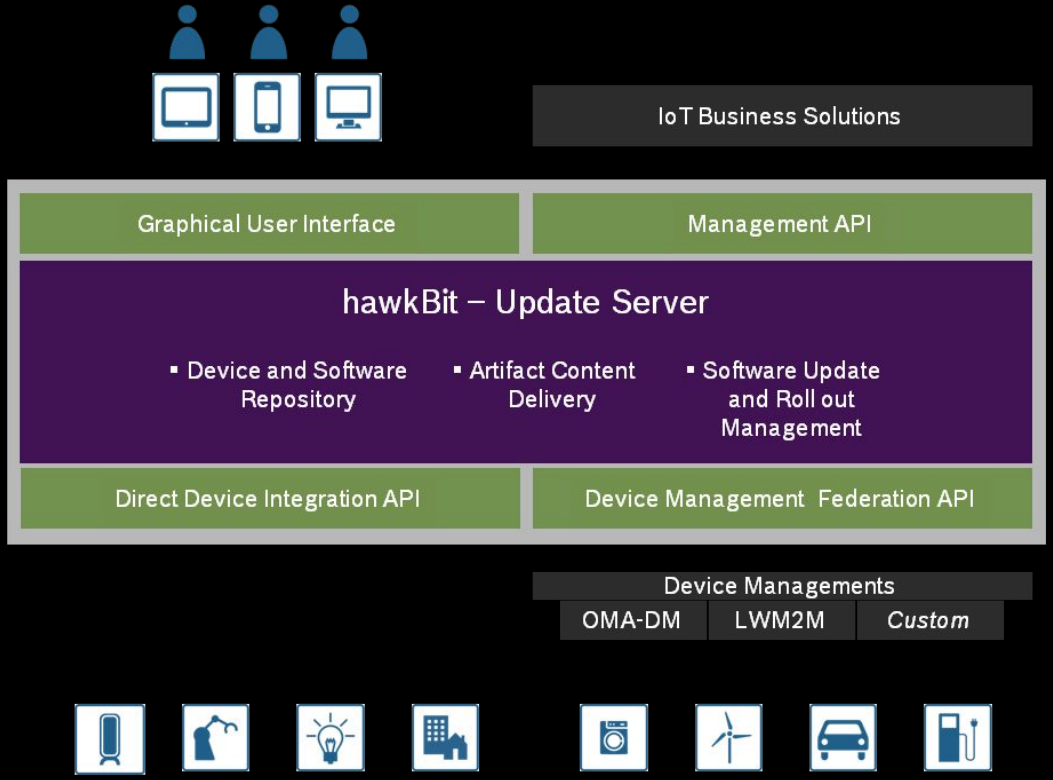
Eclipse IoT is an ecosystem of companies and individuals that are working together to establish an Internet of Things based on open technologies.

https://iot.eclipse.org, https://eclipse.org/hawkbit/

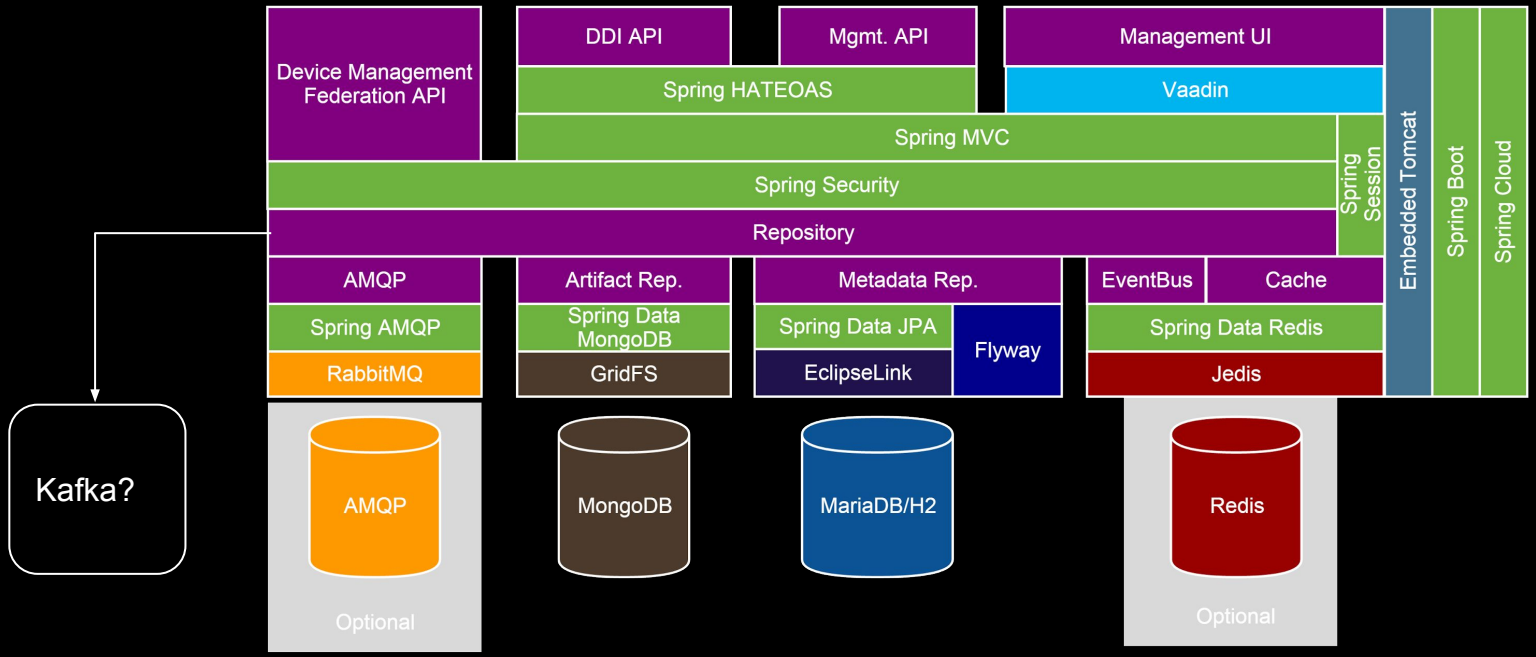
One of the (many) projects is hawkBit *"to create a domain independent back end solution for rolling out software updates to constrained edge devices connected to IP based networking infrastructure"*

hawkBit overview

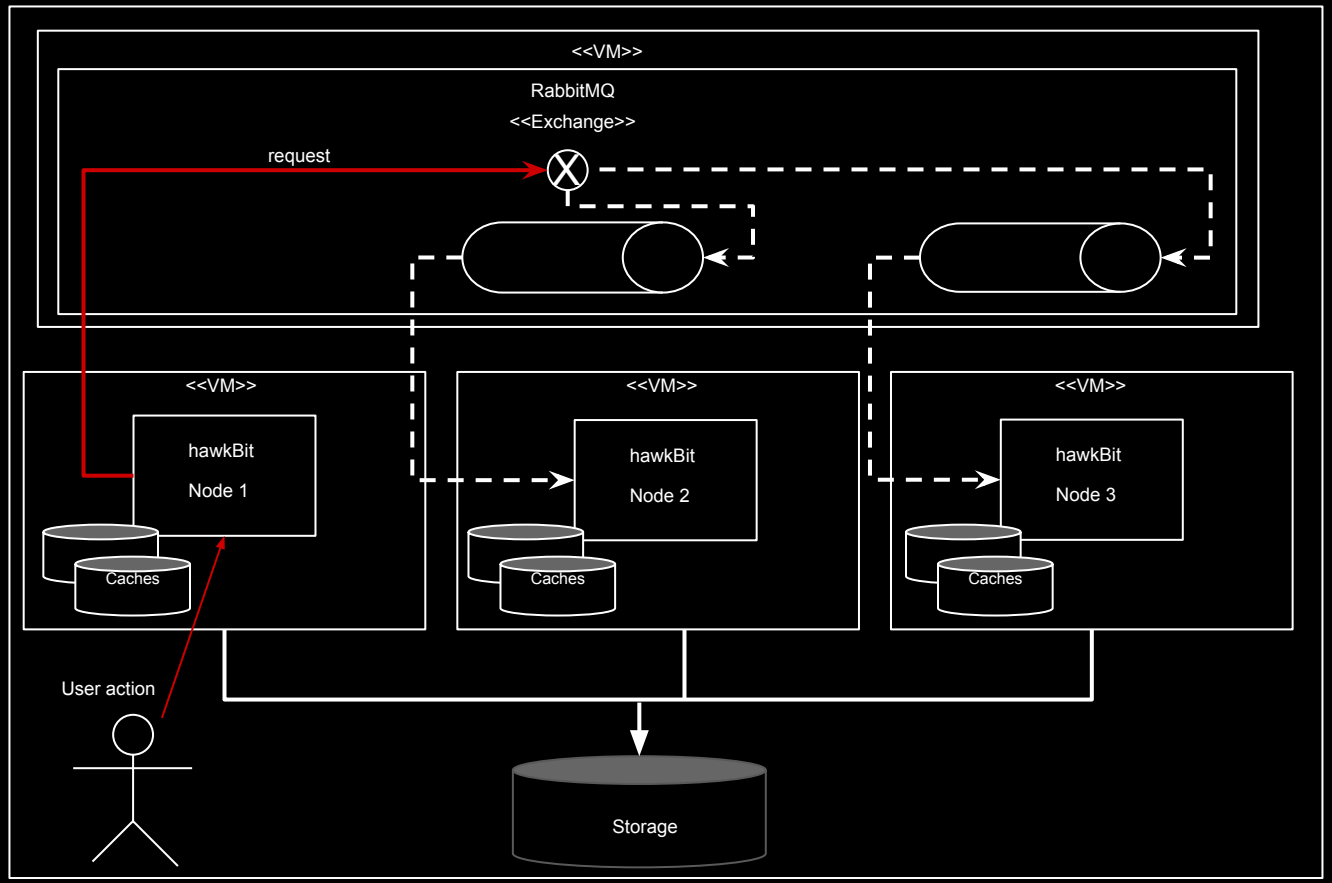
- User/Applications
  - UI
  - MGMT (API)
- Devices
  - DDI (HTTP/REST/JSON)
  - DMF (AMQP)



hawkBit Architecture



Clustering


<<VM>>
RabbitMQ
<<Exchange>>
request
<<VM>>
hawkBit
Node 1
Caches
<<VM>>
hawkBit
Node 2
Caches
<<VM>>
hawkBit
Node 3
Caches
User action
Storage

hawkBit: workflow of a rollout campaign

- Prepare the update file and upload it
- Create a Software Module and add an artifact to it
- Create a Distribution
- Rollout a distribution to Targets
- Targets features:
  - Attributes (i.e HW revision, custom)
  - Tags (for grouping purposes)
  - Others like device description, what installed, logs, etc..
- Rollouts can be managed by groups
  - TAG filter
  - Group threshold

Update Factory

Platform to manage and deliver software update artifacts which are deployed on single copy Linux and Android devices, featuring recovery mode

Or simply….

“Manage and Deploy Android-like software updates on Embedded Linux!”

Update Factory Architecture

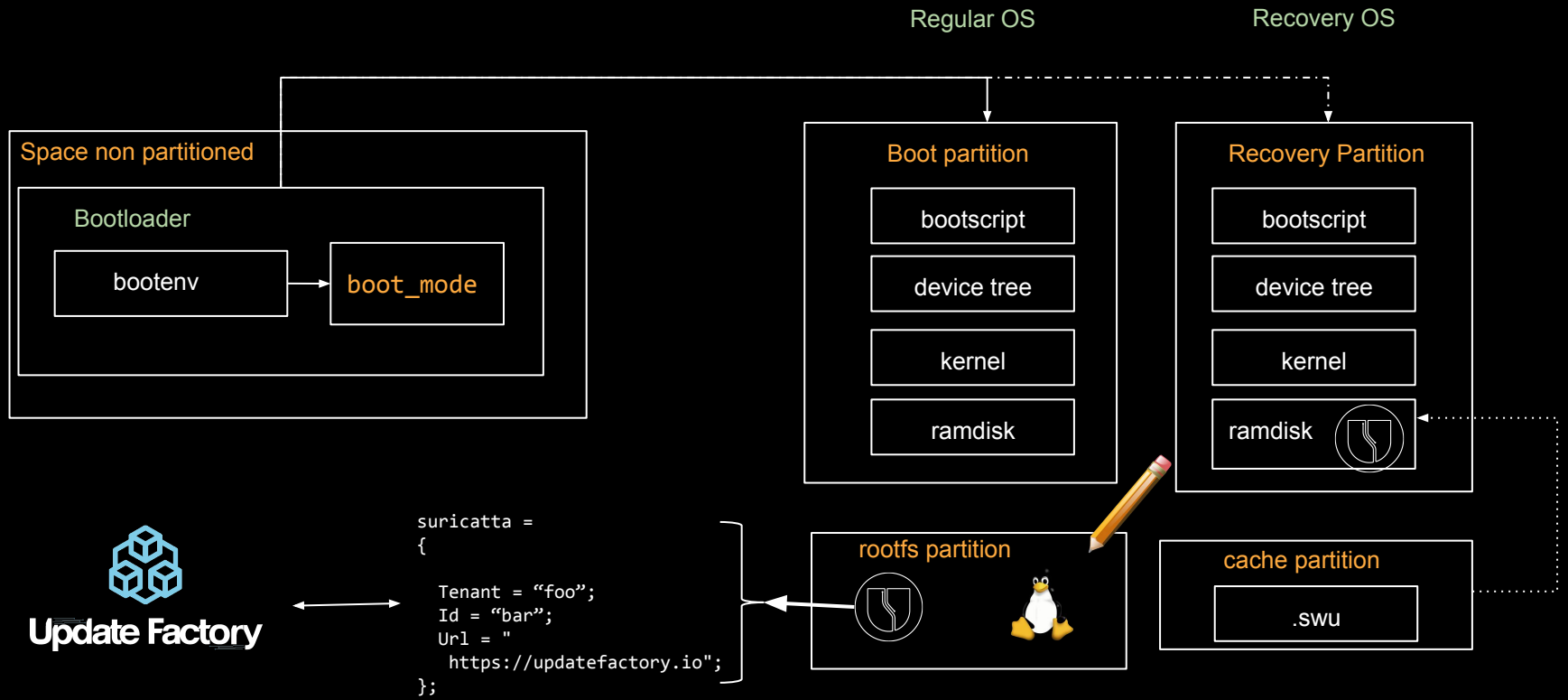
- Service on the embedded device
  - Gnu/Linux featuring SWUpdate
  - Android Service featuring Update Server API
- Update Server featuring hawkBit™
- IAM Server
- Artifact Repository
- Metadata Repository
- MsgBroker

Android “like” behaviour on Embedded Linux

Update Factory implements all the missing bits to have an Android-like OTA mechanism on an Embedded Linux OS

- Device to cloud communication
- Bootloader coordination (boot OS selection)
- Recovery partition
- Recovery bootscript
- Recovery ramdisk
- Update installation feedback to the cloud

Update Factory: Linux Update Anatomy

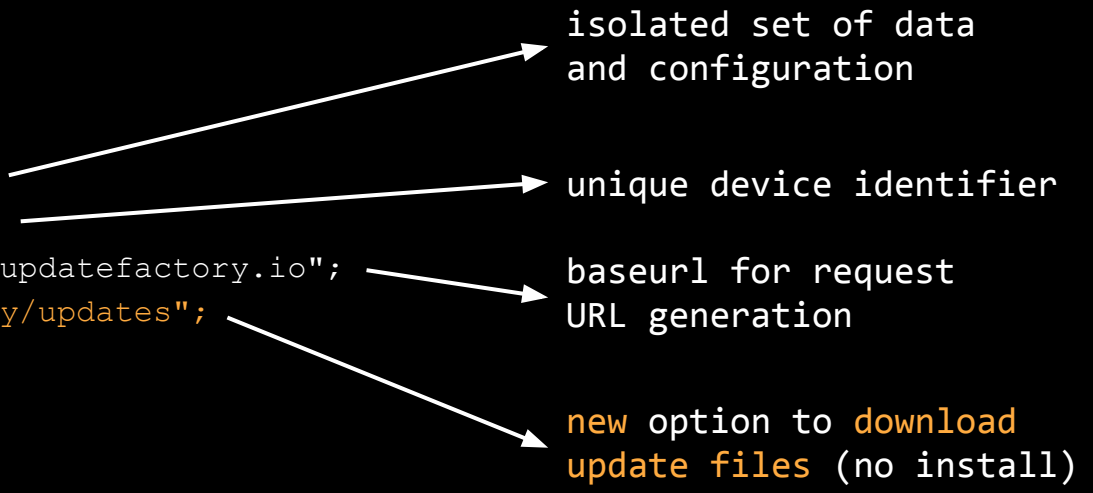


Update Factory: device to cloud

SWUpdate implements the suricatta daemon mode which polls remote update server hawkBit.

Configuration file:

```
suricatta :
{
  tenant            = "system";
  id                = "device";
  url               = "https://updatefactory.io";
  artifactsstorage = "/recovery/updates";
};
```



Update Factory: bootloader coordination

- Switch between Regular OS and Recovery OS by changing bootloader environment variables
- distro_bootcmd current U-Boot standard solution for distro booting across different boards
- if boot_mode variable is set to update force the number of the partition to boot from:

```
bootcmd=run update_bootcmd; run distro_bootcmd
update_bootcmd=if test "${boot_mode}" = "update"; then echo "Update mode selected";
setenv distro_bootpart 3; setenv scan_dev_for_boot_part run scan_dev_for_boot; fi
```

Update Factory: recovery partition

Yocto now has wic support for easier and streamlined partition creation and management.

Addition of recovery partition:

- new filescopy wic plugin to populate the partition
- .wks descriptor file
  - part --source filescopy --size 1000 --fstype=ext4 --label recovery --align 4
- “by-label” fstab entry

Update Factory: bootscript & ramdisk

Recovery bootscript loads the recovery ramdisk

```
load ${devtype} ${devnum}:${distro_bootpart} ${a_ramdisk} ${prefix}swupdate.img
bootz ${a_zImage} ${a_ramdisk} ${a_fdt}
```

Recovery OS ramdisk:

- minimal Linux OS
- SWUpdate to install update files from local storage
- filesystem utils

Update Factory: installation feedback

hawkBit server needs to know if update applied successfully.

SWUpdate suricatta daemon:

- reads ustate bootloader variable (update is installed or failed)
- provides feedback to hawkBit from Regular OS

Update Factory: future developments

- expand support to other boards and SOCs
- manual recovery mode to update from local storage (e.g. USB) if connection is broken
- store update files in separate partition / storage
- support to update Recovery OS from the Regular OS as a second step of the update process

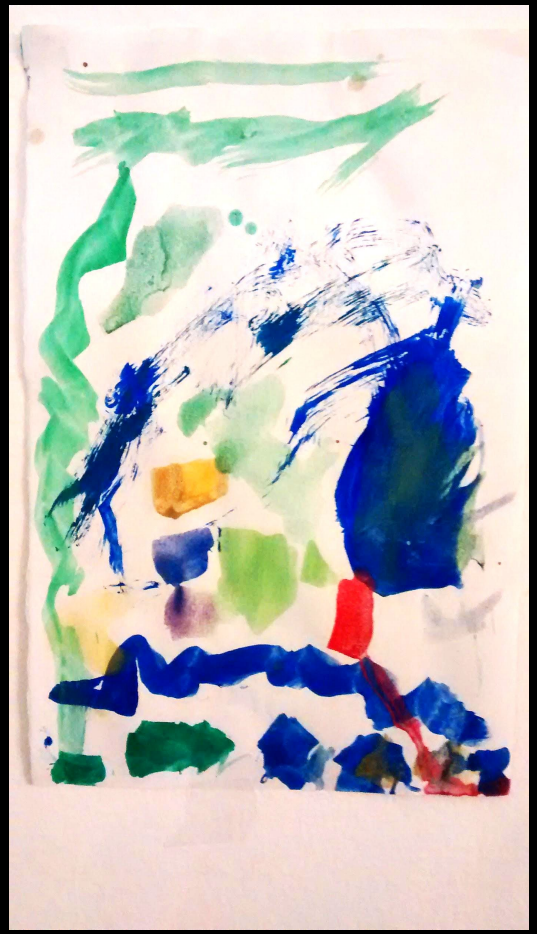
Update Factory goals

- Support medium scale general purpose CPU-SOC deployments
- Android like OTA update strategy for Embedded Linux based on single image approach
- Update core components of the system
- Provide a solid integration with Yocto Linux to facilitate the adoption
- Remote Update Management Platform as a service

Links

- https://www.kynetics.com/update-factory
- https://docs.updatefactory.io/
- https://github.com/Kynetics/meta-updatefactory
- http://warpx.io/blog/tutorial/easy-os-upgrades-swupdate

- https://eclipse.org/hawkbit/
- https://sbabic.github.io/swupdate
- https://android.googlesource.com/platform/bootable/recovery/+/android-8.0.0_r4/recovery.cpp#167



Thanks:
Nicola La Gloria, Andrea Zoleo, Will Martindale, Daniele Sergio, Roberto Sartori, Eric Nelson, Gary Bisson (Boundary Devices), Gabriel Huau (witekio) and Amit Pundir (Linaro).

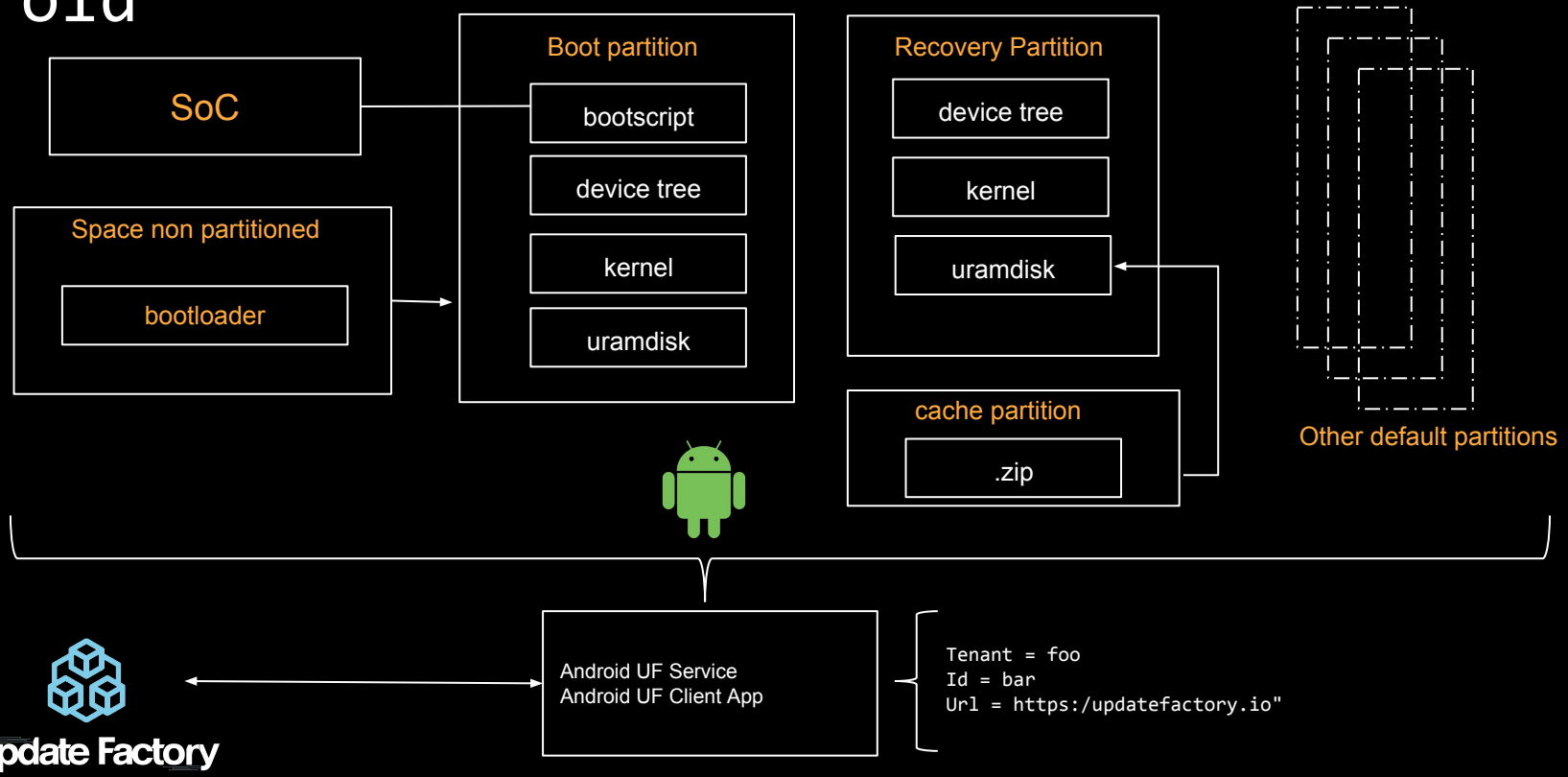
and...

Thanks to my daughter Marianna for the drawing!

Contacts:

USA	Italy
Kynetics LLC 2040 Martin Ave, Santa Clara CA 95050 Ph: +1 (408) 475 7760	Kynetics Srl Via G. Longhin, Padova (PD) 35129 Ph: +39 (049) 781 1091
info@kynetics.com | www.kynetics.com	

Android


SoC
Space non partitioned
bootloader
Boot partition
bootscript
device tree
kernel
uramdisk
Recovery Partition
device tree
kernel
uramdisk
cache partition
.zip
Other default partitions
Android UF Service
Android UF Client App
Tenant = foo
Id = bar
Url = https:/updatefactory.io"
Update Factory