Facing the Challenges of Updating Complex Systems

Putting it all together

FOSDEM 2018, Enrico Jörns, Pengutronix e.K.
About Me

- Enrico Jörns
- Embedded Software Engineer
- Pengutronix
- RAUC update framework co-maintainer
Motivation

Updating is a solved topic!..?
Motivation

testing

data

application

watchdog

init

deployment server

device

bootloader
Bootloader Support – Barebox

config → algorithm
persistent status

select

disk0.1
disk0.2

boot targets
Bootchooser Framework

- disk0.1
- disk0.2

priority: 20
attempts: 3
system0
system1
priority: 10
attempts: 3

reset: power-on
system0: disk0.1
system1: disk0.2

failed

boot
disk0.1
disk0.2

attempts --

highest priority

attempts > 0
attempts > 0

power on

attempts:=3

watchdog
reset

priority: 20
attempts: 3

priority: 10
attempts: 3

system0
system1
# X86 – Pure UEFI Boot

**BootNext:** 0001

**BootOrder:** 0001,0002

**BootEntries**

<table>
<thead>
<tr>
<th>BootEntry</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0001</td>
<td>HD(1,GPT,&lt;UUID-1&gt;/File(KernelA),rootfs=....</td>
</tr>
<tr>
<td>0002</td>
<td>HD(1,GPT,&lt;UUID-2&gt;/File(KernelA),rootfs=....</td>
</tr>
</tbody>
</table>

- **Kernel:**
  - A (blue)
  - B (green)

- **Rootfs:**
  - A (blue)
  - B (green)

- **System:**
  - A (blue)
  - B (green)
Updating The Bootloader?

eMMC

extCSD

boot0

boot1

user

boot.img

system
Updating The Bootloader?

eMMC

eMMC

boot0

boot1

user

extCSD

boot.img

system
Updating The Bootloader?

- **extCSD**
- **boot0**
- **boot1**
- **user**
- **atomic**
- **boot.img**
- **system**
- **eMMC**
Detecting Freezes – Watchdogs!

- ROM Loader
- Bootloader
- Kernel
- System

⚠️
Detecting Freezes – Watchdogs!

ROM Loader → Boot-loader → Kernel → System

start → reset → Watchdog → System reset
systemd – Watchdog Multiplexer

![Diagram showing systemd Watchdog Multiplexer with SW-Watchdogs and HW-Watchdog]

- **app1.service**
  - WatchdogSec=10

- **app2.service**
  - WatchdogSec=20

- **app2.service**
  - WatchdogSec=30

- **watchdog.conf**
  - RuntimeWatchdogSec=10
  - ShutdownWatchdogSec=300
systemd

- Central control and overview!
- Service Failure Configuration
  - Restart
  - RestartSec
  - ...
- Watchdog Multiplexerer
- /system-update
  - bootstrapping config / data
Data Storage / Migration

Data in rootfs

1. update

2. /etc

- copy by updater!
- migration: simple
- fallback: old data!
Data Storage / Migration

Data in separate slot

- no copying
- mount to /data
- migration: simple
- fallback: tricky!
Data Storage / Migration

Data in two separate slots

- copying by updater
- migration by application
- mounting: tricky
- fallback: old data!
Updating and Trusted Boot

**dm-verity**

- **Build System**
  - image
  - hash tree
  - install
  - block device
  - r/o

**dm-integrity**

- ** Build System**
  - tar
  - extract
  - ext4
  - dm-integrity
  - journal tags
  - block device
  - r/w

**Target**
Testing Updates – Labgrid

**update-test.py**
- provide update
- trigger install
- power cycle
- test bootloader
- test linux

---

**Diagram:**

- **Labgrid**
  - ShellDriver
  - BareboxDriver
  - PowerDriver

- **HW / Qemu**
  - Bundle
  - Linux
  - Barebox
  - Power
casync

- Image updates over Network
  - Too large (slow connection)
  - Temporary storage required

→ delta updates
→ not reinvent the wheel

“casync (content-addressable synchronisation) is a Linux software utility designed to distribute frequently-updated file system images over the Internet.”

[Wikipedia]
casync – Chunking

- block device / directory tree
- serialized stream
- hashing (ID)
- compressing

index file
.chunkstore

.hashing (ID)
casync – Extracting

chunk store

https

.index file

.serialized stream

.block device / directory tree
casync – RAUC

-.caidx
metadata

update

chunk store

install

slot A

seed store

slot B
Field Deployment

update
HawkBit – Deployment Server

- Web UI
- Management API
- Device Integration API
Field Deployment – HawkBit
Field Deployment – HawkBit

group 1

group 2

group 3

error threshold
Field Deployment – HawkBit

error threshold

stop!
Conclusion

• Update Frameworks cannot provide full solutions
• Not just stacking components
• Fine-grained configuration
• Updating is highly use-case specific
Questions?
Links

- github.com/rauc
- rauc.readthedocs.io
- github.com/systemd/casync
- github.com/labgrid-project/labgrid
- github.com/eclipse/hawkbit