

Implementing Power-safe Atomic Over the Air Updates

Presented by
Toradex



Implementing Power-safe Atomic Over the Air Updates



Presented by
Drew Moseley
Technical Solutions Architect
Toradex

WITH YOU TODAY...



Drew Moseley

Technical Solutions Architect
Toradex

WE'RE LOCATED IN LUCERNE, SWITZERLAND

WHAT WE DO



Arm® System on Modules
Reliable
Long-term maintenance
Scalable
From stock



Production-ready software
Yocto-based Linux
Windows Embedded Compact
Development tools
Long-term maintenance



Ease-of-use
Support
Ecosystem

• About.me

- Embedded Linux Engineer
- 25 years experience
- Solutions Architect for the Torizon Platform

- drew.moseley@toradex.com
- <https://twitter.com/drewmoseley>
- <https://www.linkedin.com/in/drewmoseley>
- <https://toradex.com/torizon>

Agenda

- OTA & OSTree Background
 - Power safe definition
 - Architecture discussion
 - Demo
- 


Working on updates 0% complete.
Don't turn off your PC. This will take a while.

Updates Suck!



About 11 minutes remaining



Package dependencies cannot be resolved

This error could be caused by required additional software packages which are missing or not installable. Furthermore there could be a conflict between software packages which are not allowed to be installed at the same time.

▼ Details

The following packages have unmet dependencies:

libqt5dbus5: Depends: qtbase-abi-5-6-1 but it is a virtual package
libqt5network5: Depends: qtbase-abi-5-6-1 but it is a virtual package
Depends: zlib1g (>= 1:1.1.4) but 1:1.2.8.dfsg-2+b3 is to be installed
libqt5qml5: Depends: qtbase-abi-5-6-1 but it is a virtual package
libqt5sql5: Depends: qtbase-abi-5-6-1 but it is a virtual package
libqt5sql5-sqlite: Depends: qtbase-abi-5-6-1 but it is a virtual package
libqt5xml5: Depends: qtbase-abi-5-6-1 but it is a virtual package
qtcreator: Depends: qml-module-qtquick-controls (>= 5.5.0~) but 5.6.1-3 is to be installed
Depends: qml-module-qtquick2 (>= 5.5.0~) but 5.6.1-11 is to be installed
Depends: qtcreator-data (= 4.1.0-3) but 4.1.0-3 is to be installed
Depends: libgcc1 (>= 1:3.0) but 1:6.2.0-10 is to be installed
Depends: libqt5concurrent5 (>= 5.6.0~rc) but 5.6.1+dfsg-3+b1 is to be installed
Depends: libqt5core5a (>= 5.6.1) but 5.6.1+dfsg-3+b1 is to be installed
Depends: libqt5designer5 (>= 5.6.0~beta) but 5.6.1-4 is to be installed
Depends: libqt5designercomponents5 (>= 5.6.0~beta) but 5.6.1-4 is to be installed
Depends: libqt5gui5 (>= 5.5.0~) but 5.6.1+dfsg-3+b1 is to be installed

OK



Your Windows Update failed. But don't worry. We can help.

SO WHY DO WE CARE?

- Kernel patches
- Drivers
- New hardware support
- Firmware binaries
- Vendor updates (things like Spectre, Meltdown workarounds)
- Security patches for user-space libraries like SSL (think HeartBleed), message-frameworks, etc.
- Feature updates
- Bug fixes



WHAT IS OSTREE?

"libostree is both a shared library and suite of command line tools that combines a “git-like” model for committing and downloading bootable filesystem trees, along with a layer for deploying them and managing the bootloader configuration."¹

- "git-like" model
- bootable filesystem trees
- Bootloader configuration

¹ <https://github.com/ostreedev/ostree#libostree>



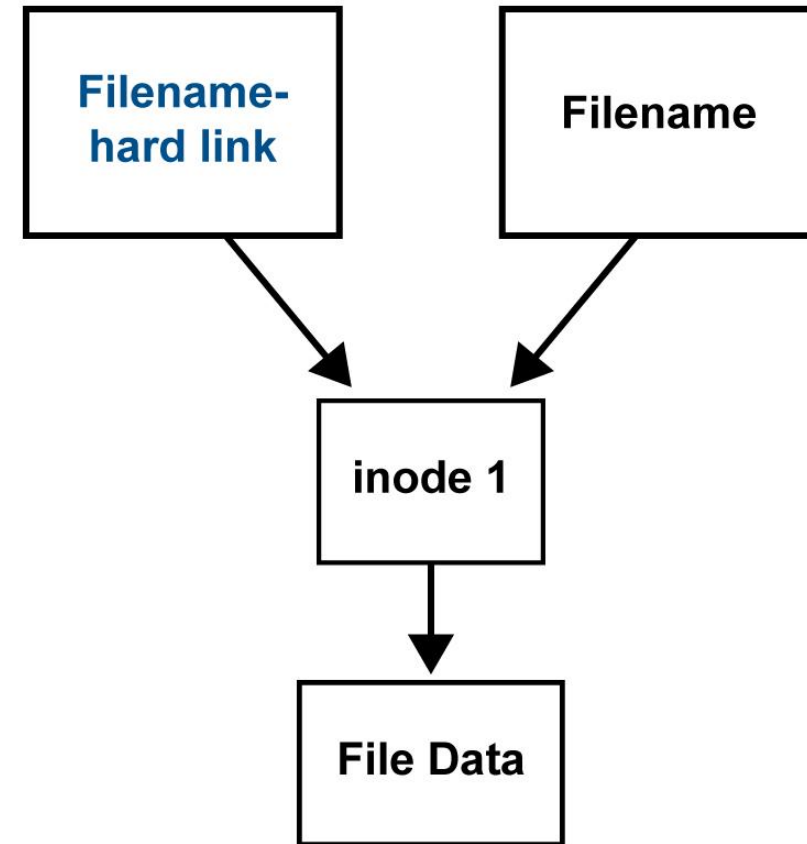
OSTREE IN A NUTSHELL

- Files are:
 - › stored, indexed by checksum, in content-addressable form.
 - › checked out via hard links
 - › immutable (ie read-only)
- Provides a mechanism to commit and checkout branches (or "refs").
- Manages bootloader configuration via **The Boot Loader Specification**
 - › (GRUB and U-Boot supported)
- Operates in userspace via a library and CLI tools
- Works on top of any Linux filesystem.
 - › As long as it supports hard links.

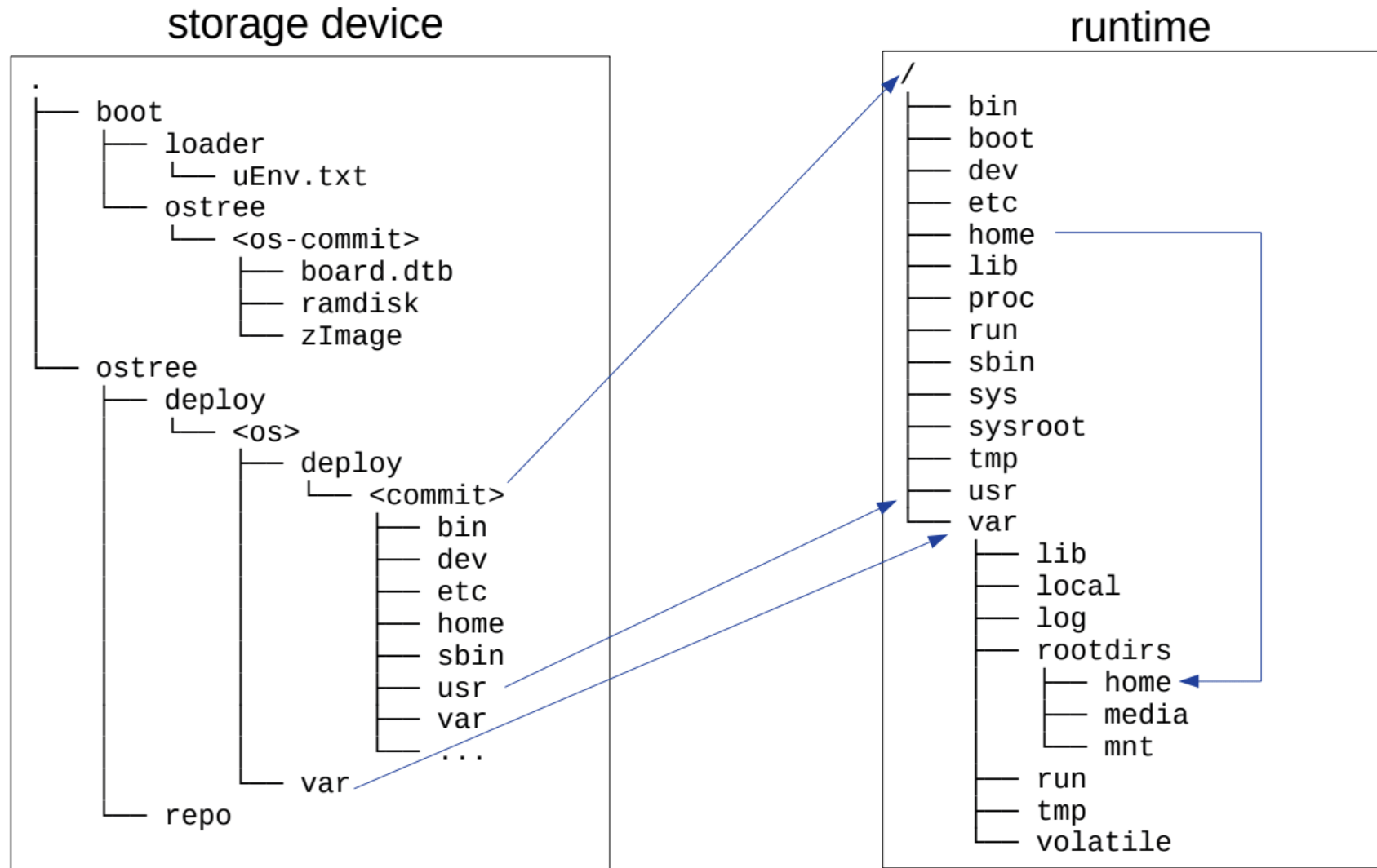
¹ <https://www.freedesktop.org/wiki/Specifications/BootLoaderSpec/>

BASICS

- File based (!)
- Relies on non-root mount/“bind-mount”
 - › Normally the root of a file system is mounted as “the root”
 - › Linux allows to bind mount a subdirectory
- Initramfs mounts OSTree
 - › Pivot into bind mount/sub-directory
- Hardlinks are used to speed-up deployment and minimize space usage



OSTREE FILESYSTEM LAYOUT (SIMPLIFIED)



USERS

- Fedora CoreOS, Fedora Silverblue, Fedora IoT
- Endless OS – Debian based distribution
- meta-updater – OpenEmbedded meta layer using OSTree
 - › TorizonCore (by Toradex)
 - › Automotive Grade Linux
 - › Linux Microplatform
 - › Full Metal Update
 - › EdgeHog
- Package management systems: rpm-ostree and flatpak

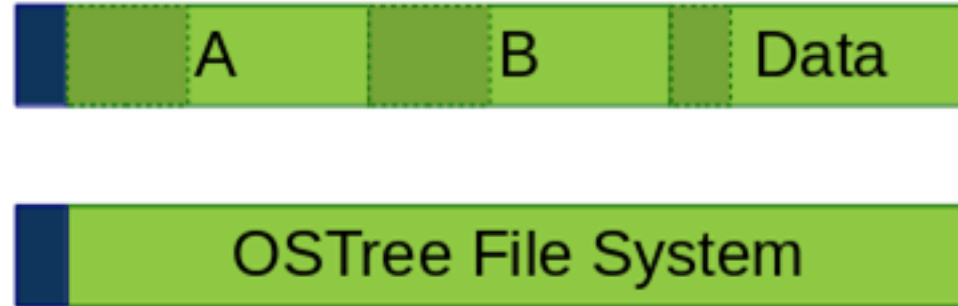
ALTERNATIVES

- A-B / Dual Bank
 - › Block-based
- Package Manager
 - › Package-based
- System Containers
 - › Container-based



ADVANTAGES

- Space savings
 - › Including automatic de-duplication
- Minimal update size
 - › Diff updates of per-file changes
- Integrity can be verified
- Atomic updates
- Immutability & Revision Control



WHAT IS POWER SAFETY?

Devices are kept in uncontrolled, hostile environments

- Network attackers
- Unrestricted physical access to unknown people
- Limited/no access by operations staff

Power can be removed at any time

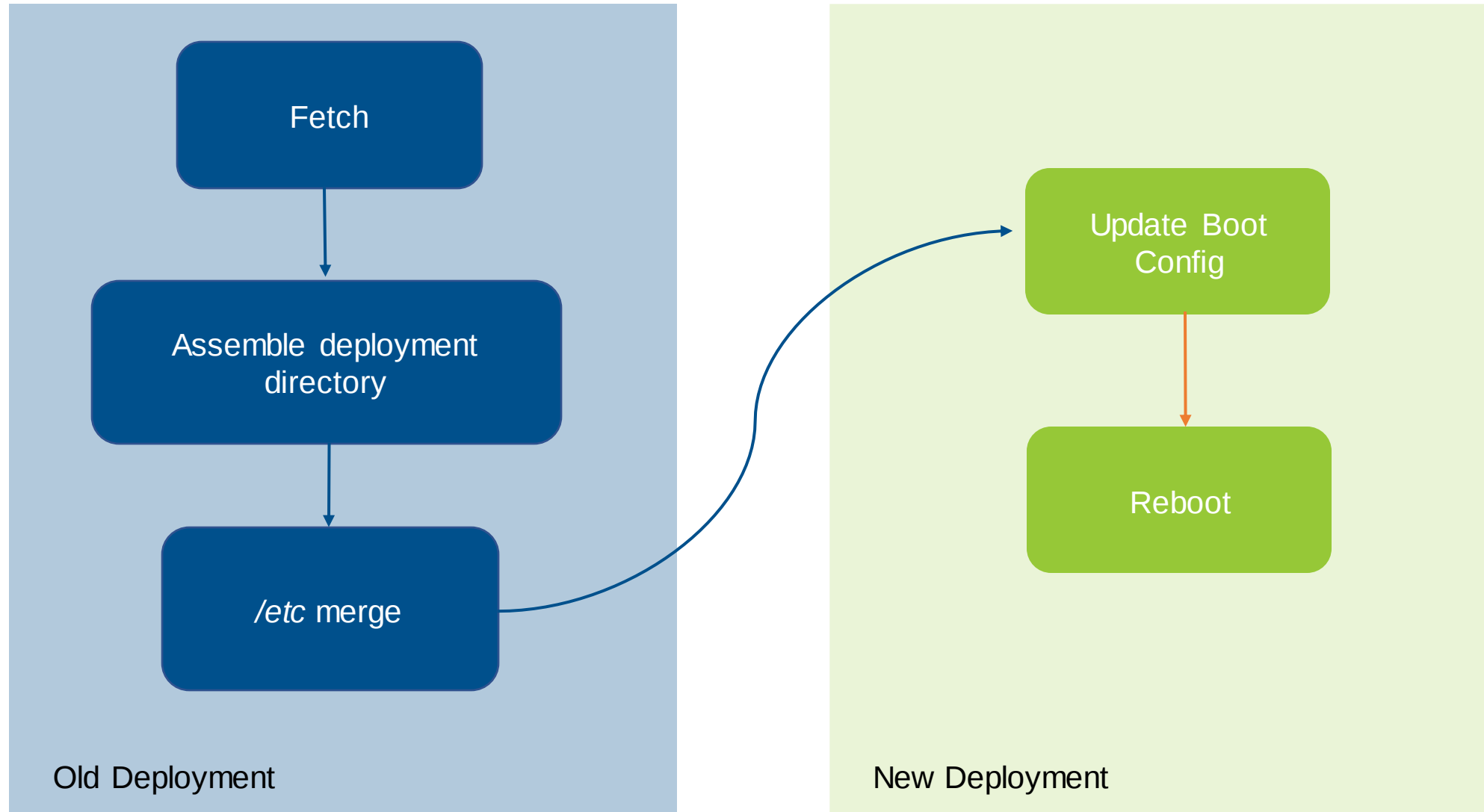
- Need to ensure atomic operations
- Avoid bricked (i.e. unbootable) devices in the field

OTA system must:

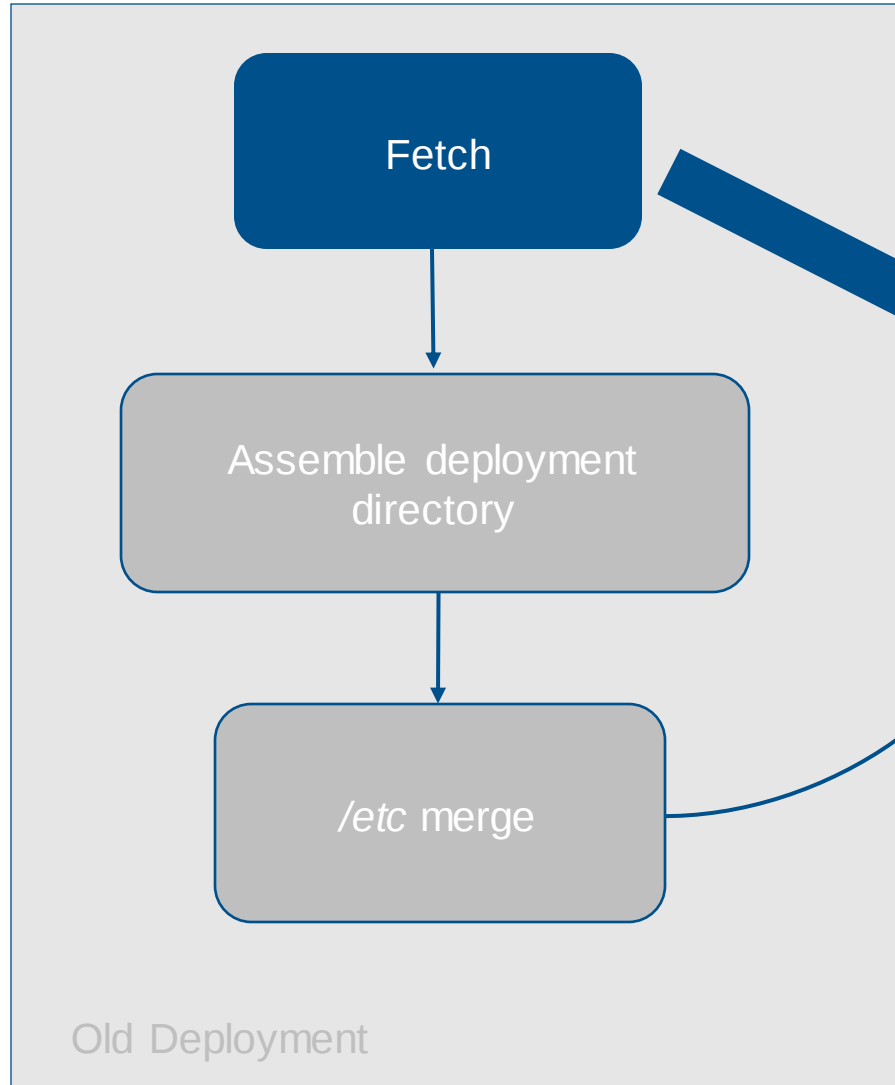
- Detect and mitigate download failures
- Handle OS changes as an atomic operation
- Automate rollback when detecting issues



OSTree UPDATE STATES



FETCH STATE



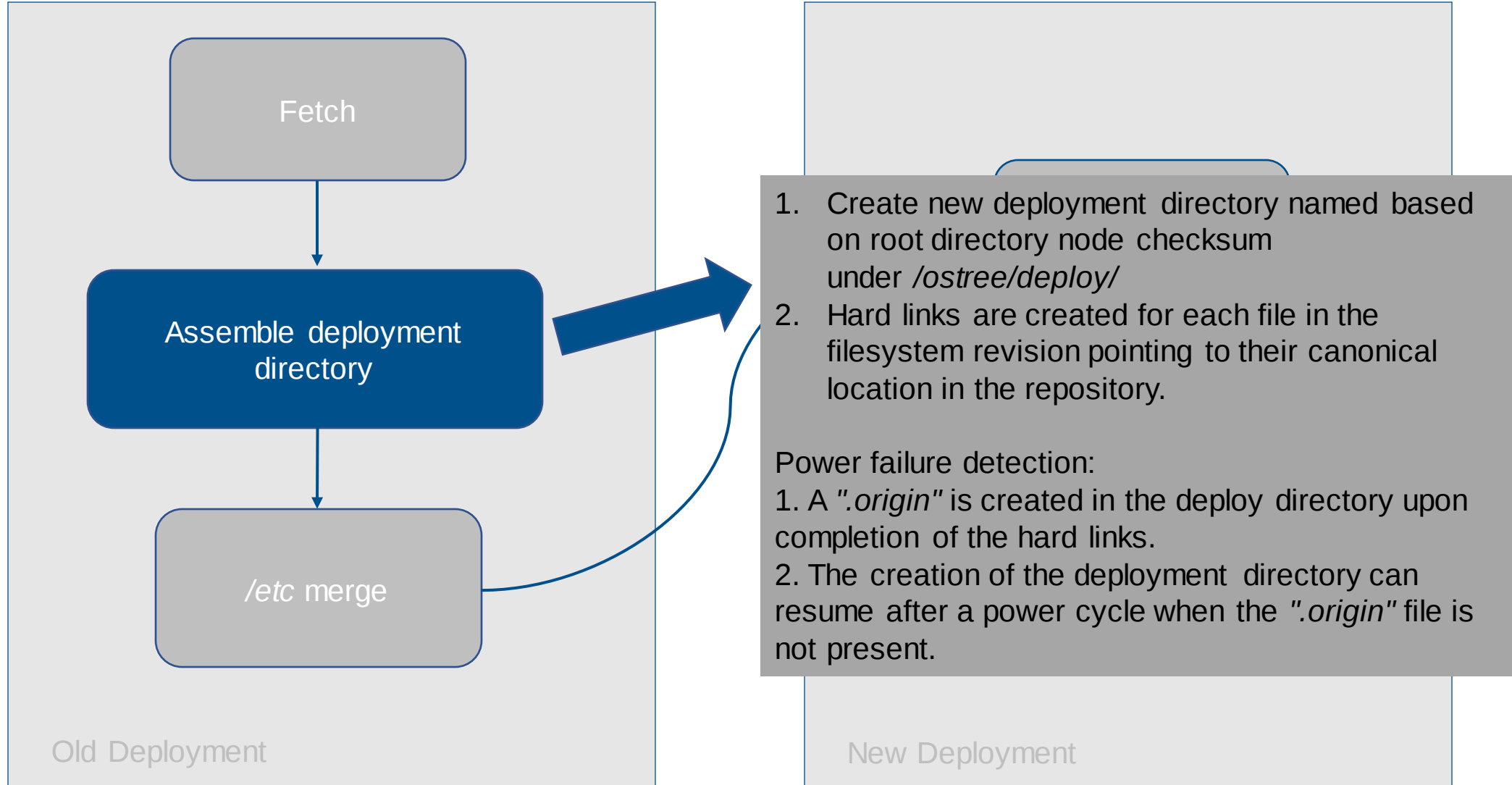
1. All new objects fetched over HTTP
2. Zlib compression
3. Existing objects can be reused
4. Checksum verified
5. Objects stored in `/ostree/repo/objects/`
6. Binary delta can be enabled at the per-file level

Power failure detection:

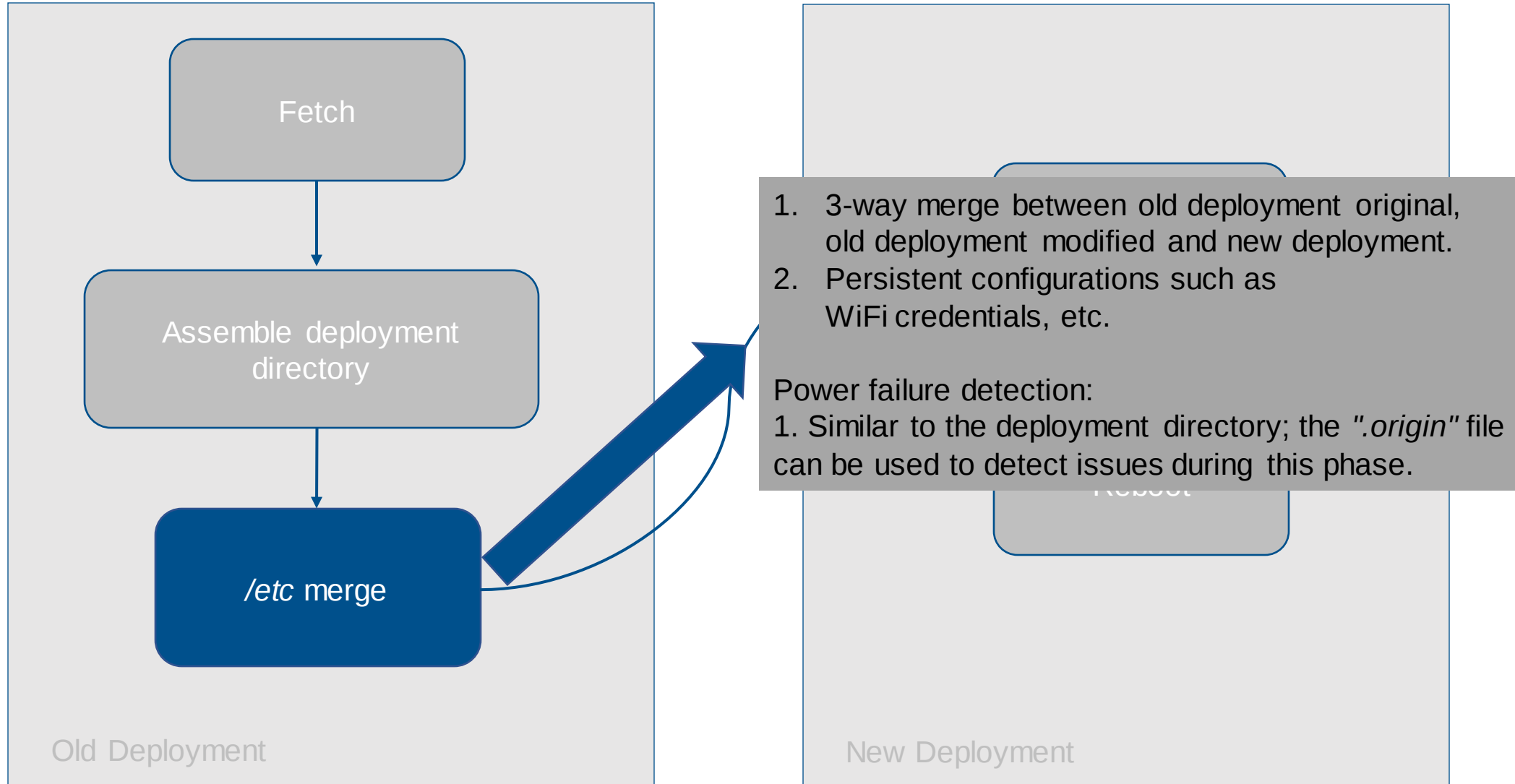
1. Objects are fetched to a staging location whose name is based on the current boot ID.
2. After successful fetch of all objects, they are moved out of staging and then the staging area cleaned up.
3. Any staging directories for unknown boot IDs are assumed incomplete and pruned.
4. Active deployments must be re-downloaded.

New Deployment

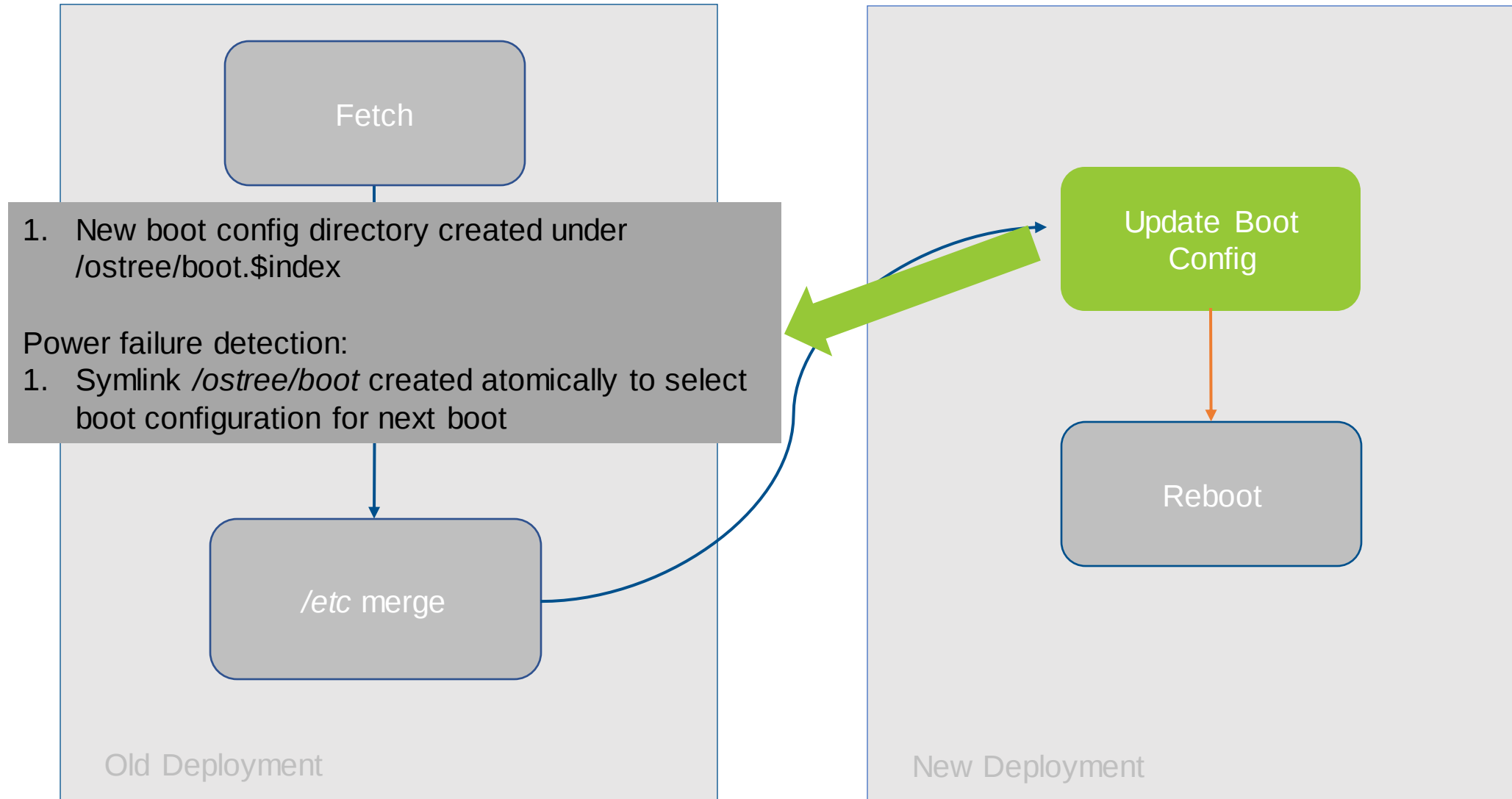
ASSEMBLE STATE



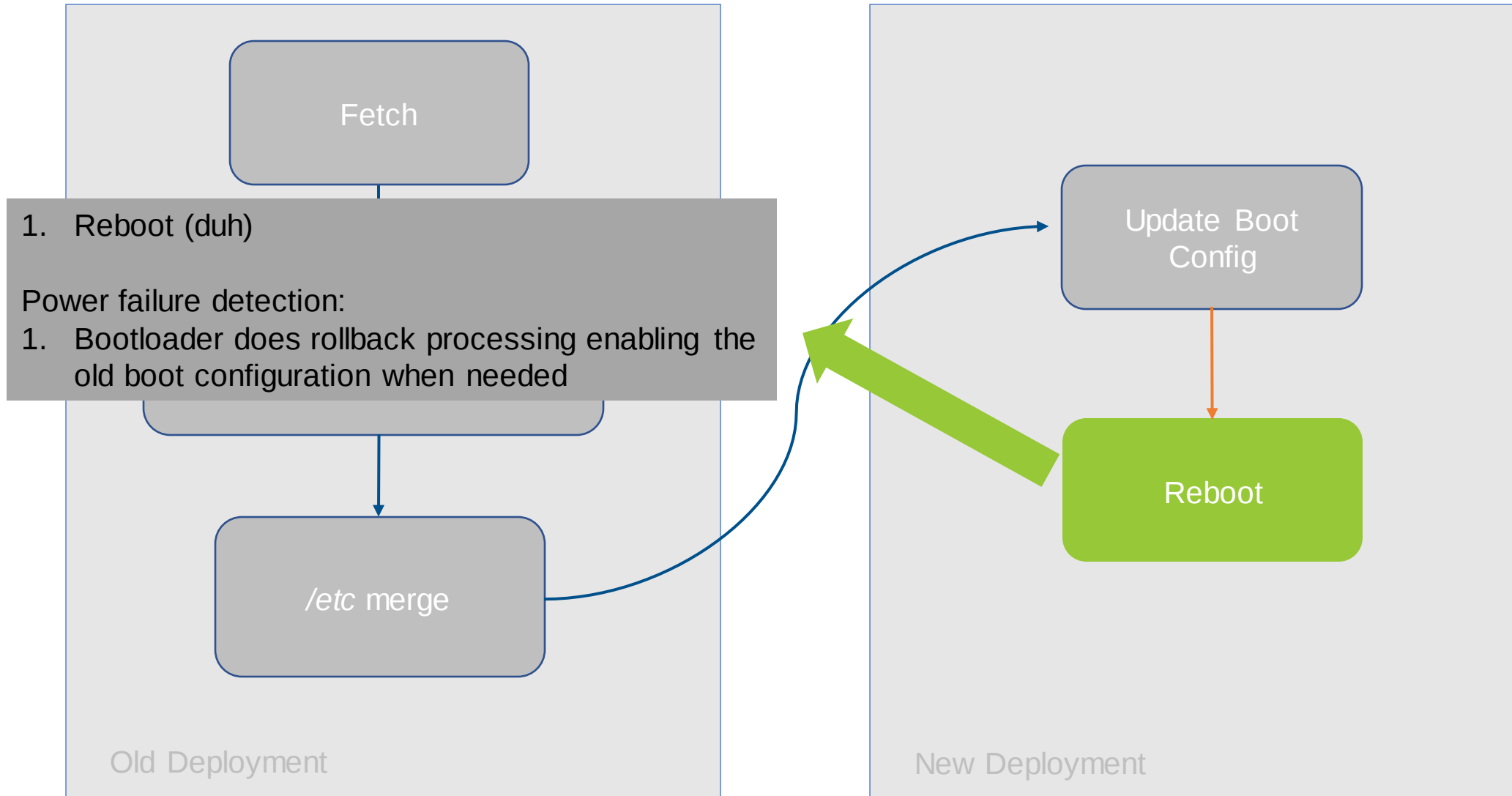
MERGE STATE



MERGE STATE



MERGE STATE





Demo Time

REFERENCES

- OSTree - Read the Docs:
 - › <https://ostree.readthedocs.io/>
- meta-updater:
 - › <https://github.com/advancedtelematic/meta-updater>
- Toradex Developer Documentation:
 - › <https://developer.toradex.com/knowledge-base/ostree>
- Torizon OTA:
 - › <https://labs.toradex.com/projects/torizon-over-the-air>
- Toradex blog post:
 - › <https://www.toradex.com/pt-br/blog/is-torizon-ota-safe-for-power-loss>
- OSTree Atomic Upgrade docs:
 - › <https://ostreedev.github.io/ostree/atomic-upgrades>



Q&A





THANK YOU
FOR YOUR INTEREST

www.toradex.com
developer.toradex.com
community.toradex.com
labs.toradex.com



Torizon™



Arm® System on Modules