OTA updates done right: safe firmware delivery at scale

26 October 2026 · 5 min read · blogs.iictp.org/ota-firmware-updates-done-right

Over-the-air (OTA) updates let you fix and improve devices after they ship. They are also the most dangerous thing you do to a fleet: a bad update can brick thousands of devices at once.

TL;DR The short version

- Over-the-air updates let you fix devices after they ship, but a bad one can brick thousands at once.
- Require signed images that devices verify, and a rollback to the previous version.
- Roll out gradually from a bench to a small share of the fleet, and plan for weak links, low battery and limited storage.

Read online, listen to it, or change the text size: https://blogs.iictp.org/ota-firmware-updates-done-right

Requirements

- **Signed images,** verified by the device before use.
- **Rollback:** keep the previous version and return to it if the new one fails.
- **Atomic updates,** so a power cut mid-update cannot leave a half-written device.
- **Version checks,** to stop downgrade attacks.

Rolling out

1. Test on a bench and on a small internal group.
2. Release to a small share of the fleet and watch health.
3. Widen in stages; pause automatically on failures.
4. Keep the ability to stop an update quickly.

Plan for the field

Devices have weak or intermittent links, low battery and limited storage. Make downloads resumable, schedule them for safe moments and report status back.

Related credential: IoT & Embedded Systems Practitioner. Explore the exam facts and syllabus.

Sources and further reading

1. IETF RFC 9019. A Firmware Update Architecture for Internet of Things. rfc-editor.org/rfc/rfc9019.

Published by IICTP, an independent technical credential body, on 26 October 2026. The current version of this post is at https://blogs.iictp.org/ota-firmware-updates-done-right. More guides: blogs.iictp.org.