THE NIGHTMARE OF BUILDING AN

OTA UPDATE INFRASTRUCTURE

FOR EMBEDDED DEVICES

7 CHALLENGES
to overcome when setting up the infrastructure to provide over-the-air (OTA) firmware and application updates.

EMTERIA

THE DREAD of

UNSUITABLE HARDWARE

To initially allow OTA updates the embedded device must be able to connect to the internet and the device's processing capabilities have to be strong enough.

THE FEAR of

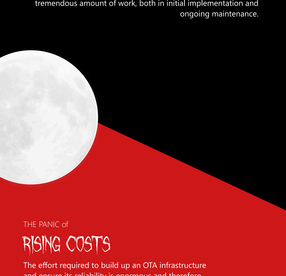
INSUFFICIENT SOFTWARE

Before getting started, it must be ensured that the code can handle updates automatically and is lightweight enough to fit on the embedded device.

THE NIGHTMARE of

UNSCHEDULED UPDATES

Automatic updates could force embedded devices and whole device fleets to interrupt their main function to perform an update. Scheduled OTA updates are only deployed and installed when the devices are freed from their regular tasks to avoid interrupting device operation.



THE TERROR of

FAILED OR INTERRUPTED UPDATES

An update should be performed in such a way that the functionality of the device can be restored in case it fails. This should be done quickly and easily without interrupting operational work.

THE THREAT of

SECURITY RISKS

OTA update functionality comes with security risks. Authentication and encrypted communication channels ensure that only verified updates are used and that the code is not changed during transmission.

THE HORROR of

NON-SCALABLE INFRASTRUCTURE

Building a scalable back-end cloud infrastructure which can handle hundreds or thousands of device connections requires a tremendous amount of work, both in initial implementation and ongoing maintenance.

THE PANIC of

RISING COSTS

The effort required to build up an OTA infrastructure and ensure its reliability is enormous and therefore particularly expensive.

EMTERIA helps you to overcome

THE 7 CHALLENGES

of setting up the infrastructure to provide OTA firmware and application updates.

CONTACT US
Gerrit Meyer
sales@emteria.com
www.emteria.com