# Secure Update Framework for Embedded Devices


Student

**Carlo Kirchmeier**


Problem: Embedded and industrial devices increasingly face strict regulatory requirements and a rapidly evolving threat landscape, yet many lack secure, standardized firmware update mechanisms. Existing solutions are often tailored to embedded Linux or relatively powerful systems and do not adequately address the needs of highly resource-constrained devices.
This leaves a large number of devices vulnerable to attacks, unreliable update processes, and operational risks caused by failed or unsafe firmware updates.

Objective: The objective of this project was to design a generalized, secure, and scalable firmware update framework suitable for a wide range of embedded and industrial devices, including highly resource-constrained hardware. A prestudy identified the most critical challenges developers face when implementing secure firmware updates as:

- Resource constraints: limited processing power, memory, and storage that restrict the use of conventional cryptographic protocols and update mechanisms.
- Robustness and reliability: high availability requirements and the need to prevent device failure or bricking during interrupted or faulty update processes.
- Ease of use: the necessity for update mechanisms that can be safely operated by non-specialized users and maintained efficiently at scale.

The designed solution therefore aims to address these challenges by providing a lightweight yet secure update mechanism, a robust architecture, and a developer-friendly integration approach that allows the framework to be adapted to diverse device capabilities and deployment scenarios.

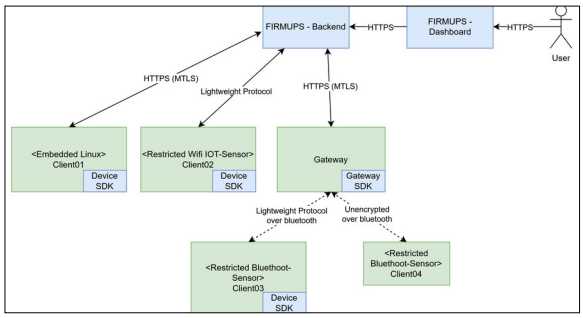
Result: The outcome of this project is the design and proof-of-concept implementation of FIRMUPS (Firmware Updates for Embedded Devices), a generalized framework for secure firmware update management in embedded and industrial environments.

To address resource constraints, a lightweight communication protocol based on CBOR and COSE was developed. Robustness and reliability are ensured through integration into already existing bootloader solutions, preventing device failure during interrupted or faulty update processes. Ease of integration is achieved through a C-based device SDK that abstracts communication, security, and update handling from device-specific logic.

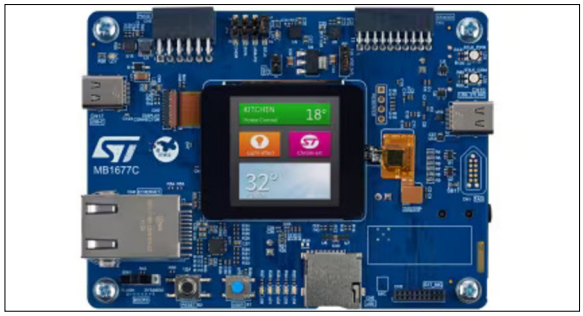
A proof-of-concept implementation demonstrates the feasibility of the architecture by securely updating a resource-constrained device running Zephyr RTOS and MCUboot.

Overall, the project provides a validated architectural foundation for secure firmware updates and establishes a solid basis for future extension toward a production-ready system.

**Architecture of the FIRMUPS system**
Own presentment




**Development kit (STM32H573I-DK) used to test proof-of-concept**
https://www.st.com/en/evaluation-tools/stm32h573i-dk.html





Advisor
**Prof. Dr. Daniel Patrick Politze**


Subject Area
**Sensor, Actuator and Communication Systems**