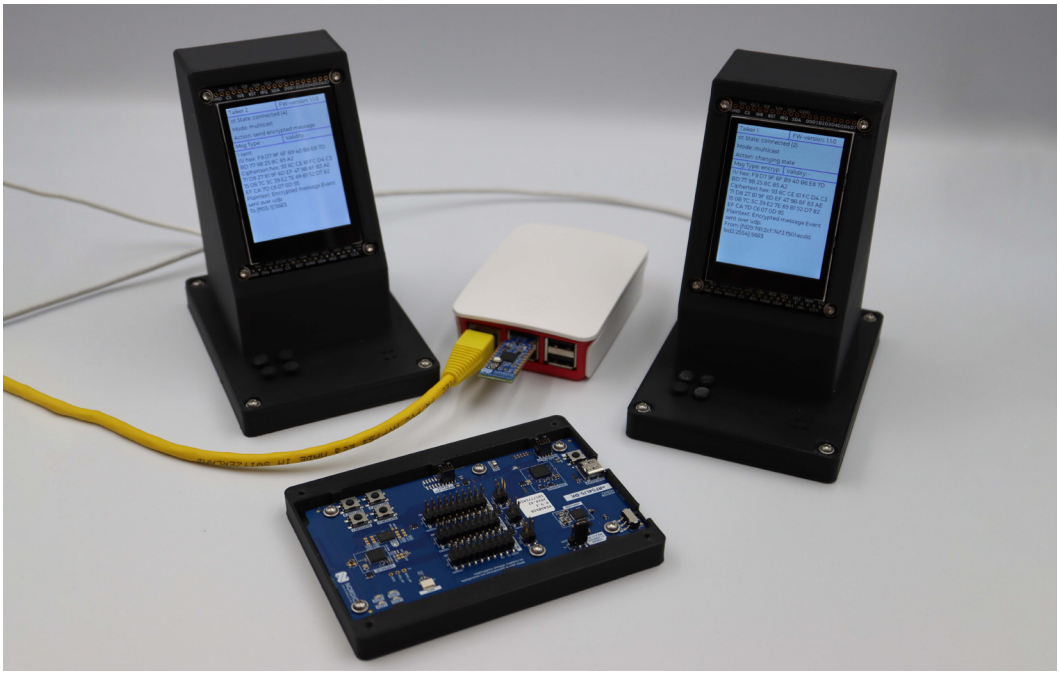
School of Engineering

Institute of Embedded Systems

Security Features of the ARM Cortex-M33



- ARM TrustZone separates memory into Secure and Non-Secure Worlds
- MCUboot verifies firmware at boot and enables secure updates
- Trusted Firmware-M provides cryptographic and security services
- Wireless firmware updates via the Thread mesh network
- The application runs on Zephyr RTOS in the Non-Secure World

Bachelor Thesis
Authors: Martin Koloska, Jerome Bassand
Supervisor: Dr. Simon Künzli
www.zhaw.ch/ines