Motivation
IoT manufacturers employ a wide range of protection technologies to keep their devices secure. Unfortunately, bugs and misconfigurations still lead to remote exploits. Attack-resilient IoT devices may use hard- and software mechanisms to detect and recover from such exploits and are capable of providing their remote backend proof that legit software is running.

Task Description
In the course of this thesis, an attack-resilient platform will be designed, implemented and analysed on a very recent ARMv8 Cortex-M microcontroller with the ARM TrustZone. The goal is to propose a combination of hard- and software mechanisms to allow the detection and recovery from compromised firmware. This includes the understanding and further development of the novel and promising CyReP architecture\(^1\), and the systematic protection of security-related code and secrets.

Requirements
- Most important: Motivation to work in the field of microcontrollers
- Good C programming skills and basic experiences with microcontroller programming
- Ability to work independent and goal-oriented
- Optional: Experience with microcontroller/ARM security features

Contact
Stefan Hristozov (stefan.hristozov@aisec.fraunhofer.de) or
Manuel Huber (manuel.huber@aisec.fraunhofer.de)
Fraunhofer Research Institute AISEC
Parkring 4, 85748 Garching (bei München)
Phone: 089/3229986157

\(^{1}\)https://www.microsoft.com/en-us/research/publication/cyber-resilient-platform-requirements/