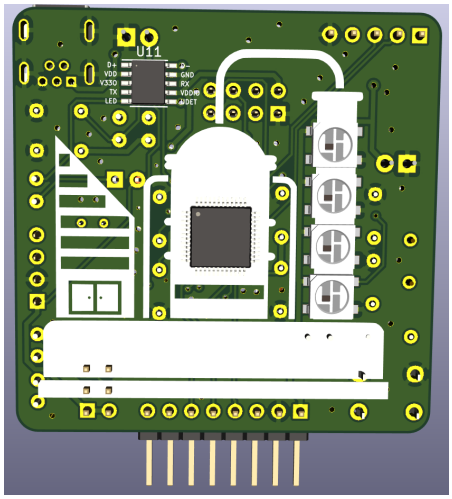
Master Thesis
Safety Aware OTA Updates for Smart Factories

Updating embedded systems reliably and robustly is challenging due their constrained nature. This is especially true in context of Smart Factories, in which in addition to security requirements also safety concerns come into play. In addition to the cryptographic verification prior to engaging a system update, factory modules have to verify that all conditions to maintain safety during the update process are met. The goal of the proposed thesis is to implement device management and OTA updates for RIOT on top of SUIT and LWM2M in a safety aware manner. For this safety requirements and attributes have to be modeled, integrated into the device management, and an safety verification step integrated into the firmware update process.

Goals of the Thesis

SUIT [1] specifies an firmware update architecture and an experimental implementation of the current draft is already implemented for the IoT Operating System RIOT [2]. By design, SUIT is agnostic to the transport of the firmware image. Combined with the device management and update management features of LWM2M, a complete OTA update solution is provided. However, adequate integration of the variety of different safety requirements often faced in Industrial IoT is not yet provided. The goal of this thesis is to fill this gap. For the evaluation, the developed solution will be deployed and tested in the Smart Factory model of the ILM learning laboratory.



An embedded system in a Smart Factory to update (symbolic image)

Project type	Master Thesis
Duration	1 Term
Language(s)	English, German
Field	Computer Science

Contact	Marian Buschsieweke
E-Mail	buschsie@ovgu.de
Room	G29-314
Tel.	+49 391 67-52673

Task

- Develop a suitable digital representation of safety attributes and states
- Extend the SUIT manifest to encode safety requirements to be fulfilled in order to proceed with the update based on the above representation
- Implement a full SUIT + LWM2M stack for a Nucleo-F767ZI using RIOT including the developed safety extensions
- Deploy the implementation in the Factory Model of the ILM Learning Laboratory
- Evaluate the implemented OTA solution:
  - Does the implementation meet the goals of the thesis?
  - What are the resource requirements of the implemented software?
  - What is the overhead of the safety additions to the OTA update sequence?
  - Measure the time the distribution of the firmware update takes experimentally in the Smart Factory model of the ILM Learning Laboratory
  - Optionally, the ComSys testbed can be used to evaluate the behavior for large scale (200 nodes) setups

References

[1] B. Moran and H. Tschofenig and D. Brown and M. Meriac. A Firmware Update Architecture for Internet of Things. Internet-Draft. `https://tools.ietf.org/html/draft-ietf-suit-architecture-12`. 2020.

[2] Emmanuel Baccelli and Oliver Hahm and Mesut Güneş and Matthias Wählisch and Thomas Schmidt. RIOT OS: Towards an OS for the Internet of Things. 32nd IEEE International Conference on Computer Communications (INFOCOM). 2013.

[3] OMA SpecWorks. Lightweight M2M (LWM2M). `https://omaspecworks.org/what-is-oma-specworks/iot/lightweight-m2m-lwm2m/` 2020.

Project type	Master Thesis		Contact	Marian Buschsieweke
Duration	1 Term		E-Mail	buschsie@ovgu.de
Language(s)	English, German		Room	G29-314
Field	Computer Science		Tel.	+49 391 67-52673