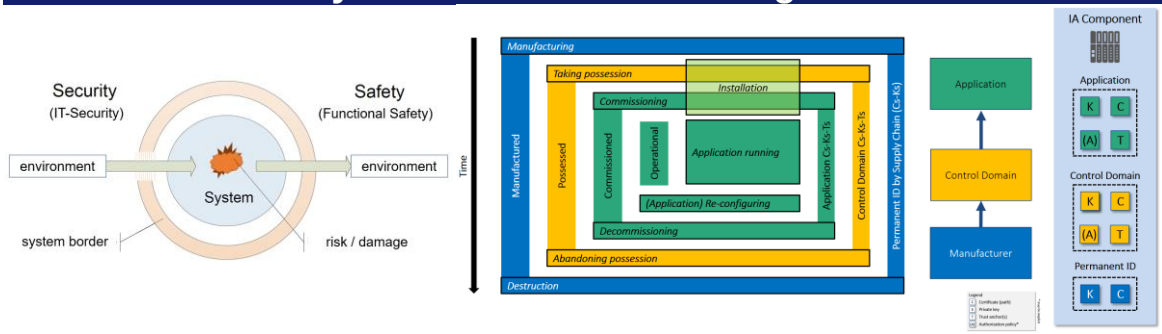
HOCH SCHULE OFFEN BURG

Forschungsmaster Applied Research

ivESK **Institut für verlässliche Embedded Systems und Kommunikationselektronik**

Embedded Security für das Internet der Dinge



Vor dem Hintergrund der jüngsten geopolitischen Veränderungen, von erfolgreichen Cyber-Angriffen und von einer aktiven Gesetzgebung auf EU- und nationaler Ebene gewinnt das Thema der Sicherheit von mikroelektronischen und eingebetteten Systemen rasch an Bedeutung.

In dem Projekt werden wir uns auf vernetzte eingebettete Geräte für das Internet der Dinge konzentrieren. Wir werden insbesondere End-to-End-Sicherheitstechnologien für ressourcenbeschränkte Netzwerke mit niedriger Datenrate und kleinen Rahmengrößen analysieren, konzipieren, implementieren und validieren, sei es für drahtgebundene Netzwerke (z.B. CAN-Bus, Modbus oder M-Bus) oder drahtlose (z.B. LPWAN-Protokolle wie LoRaWAN oder Wireless M-Bus). Diese Aktivitäten müssen auch den gesamten Lebenszyklus von Geräten und Systemen umfassen.

Hierzu soll insbesondere eine generische Sicherheitsschicht für ressourcenbeschränkte Netze spezifiziert und im Rahmen einer Referenzimplementierung und Testumgebung implementiert werden. Dabei soll auch die Frage untersucht werden, inwieweit eingebettete Geräte in der Lage sind, kryptografische Algorithmen im Rahmen von Sicherheitsprotokollen für das Internet der Dinge effizient auszuführen. Darüber hinaus erfordert die Gewährleistung der Sicherheit vernetzter eingebetteter Geräte über ihren gesamten Lebenszyklus hinweg die kontinuierliche Überwachung und Bewertung ihrer Konfiguration, was wiederum die Unterstützung durch automatisierte Werkzeuge erfordert.

Betreuer

Prof. Dr.-Ing. Axel Sikora
- axel.sikora@hs-offenburg.de
- https://www.hs-offenburg.de/sikora

Beteiligte Institute und Firmen

Das Projekt wird am **Institut für verlässliche Embedded Systems und Kommunikations-elektronik (ivESK)** durchgeführt.
- https://ivesk.hs-offenburg.de

Ziele des Projekts

- Spezifikation einer generischen Sicherheitsschicht für ressourcenbeschränkte Netze
- beispielhafte Implementierung
- Evaluation und Test

Diese Werkzeuge/Qualifikationen werden erlernt

- kryptographische Verfahren
- Sicherheitsprotokolle
- embedded Netzwerkprogrammierung
- systematische Analysen
- Methoden angewandter Forschung in realen Projekten

Literaturempfehlungen

- J. Göppert, A. Chomel, J. Sebastian, A. Sikora, "Performance Evaluation of TLS Session Establishments on an ARM Cortex-M4 Platform", 12th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, 7-9 September, 2023, Dortmund, Germany.
- A. Walz, K.-H. Niemann, J. Goeppert, K. Fischer, S. Merklin, D. Ziegler, A. Sikora, "PROFINET Security: A Look on Selected Concepts for Secure Communication in the Automation Domain", IEEE INDIN 2023, 17-20 July 2023.
- M. Skuballa, A. Walz, H. Bühler, A. Sikora, "Cryptographic Protection of Cyclic Real-Time Communication in Ethernet-Based Fieldbuses: How Much Hardware is Required?", 2021 26th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Västerås, Sweden.