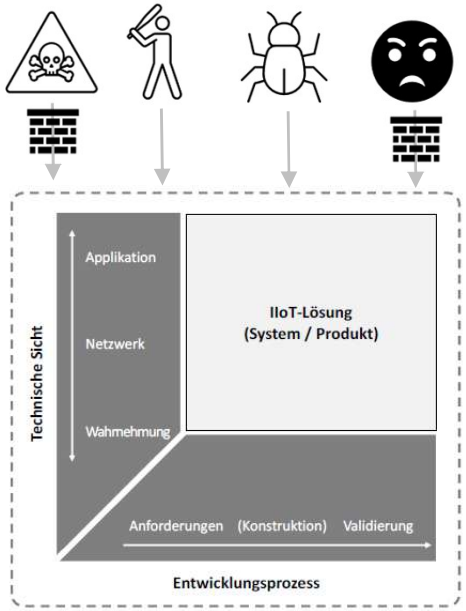
Industrial IoT (IIoT) - Aktuelle Bedrohungslandkarte und mögliche Mitigationsmaßnahmen

Fraunhofer FIT

- Der industrielle Einsatz des Internet der Dinge wird als Industrial Internet of Things (IIoT) bezeichnet. So ermöglicht z. B. das IIoT in selbstorganisierenden und selbstoptimierenden intelligenten Fabriken die Echtzeitüberwachung und -steuerung der Produktion.
- Neben vielfältigen Chancen bringt das IIoT aber auch neue IT-Sicherheitsrisiken mit sich. Der hohe Vernetzungsgrad sowie die hohe Anzahl an Heterogenität, Offenheit und Vernetzung dezentraler Produkte, Maschinen und Geräte begünstigen die Ausbreitung von Cyberangriffen und steigern das damit einhergehende Schadenspotential.
- Zur Lösung dieser emergierenden Problemstellung ist es daher notwendig, einen Überblick über mögliche und bekannte IIoT-Bedrohungen sowie damit einhergehende Mitigationsmaßnahmen herzustellen.



Forschungsfrage

- **Welche aktuellen und bekannten IIoT-Bedrohungen existieren, wie können diese geclustert werden und auf welche Komponenten im IIoT-Stack zielen diese ab?**
- **Welche Mitigationsmaßnahmen bestehen hinsichtlich dieser Bedrohungen und welche Implikationen resultieren dabei für die einzelnen IIoT-Komponenten?**

Ansprechpartner


Daniel Leuthe


Lukas Willburger

Vorgehen / Literatur

- Auswahl einer passenden Repräsentation des IIoT-Stacks und der darin enthaltenen (technischen) Komponenten
- Identifizieren von bekannten IIoT-Bedrohungen und mappen dieser zum gewählten IIoT-Stack
- Ableiten von relevanten Mitigationsmaßnahmen auf Basis der resultierenden Bedrohungen
- Kliarsky 2017: Detecting Attacks against the Internet of Things
- Berger et. al 2020: Attacks on the Industrial Internet of Things : Development of a multi-layer Taxonomy
- White Paper IEC: IoT 2020 Smart and Secure IoT Platform