Threat Analysis of Industrial Internet of Things Devices

Simon Liebl*, Leah Lathrop*, Ulrich Raithel†, Matthias Söllner*, Andreas Aßmuth*

*Technical University of Applied Sciences OTH Amberg-Weiden, Amberg, Germany
†SIPOS Aktorik GmbH, Altdorf, Germany

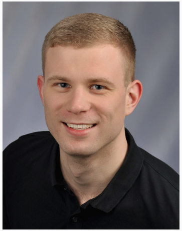
Presented by Simon Liebl <s.liebl@oth-aw.de>

October 2020

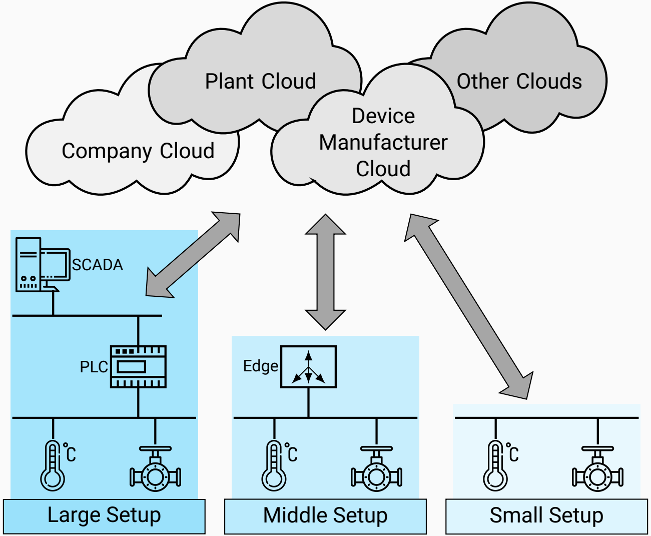
About the Presenter

Simon Liebl, M.Eng.:

- Research Assistant at OTH Amberg-Weiden, Germany
- PhD Student at Abertay University, Dundee, Scotland
- Fields of Research:
  - Industrial IoT Security
  - Hardware Security
  - Lightweight Cryptography



Industrial Internet of Things



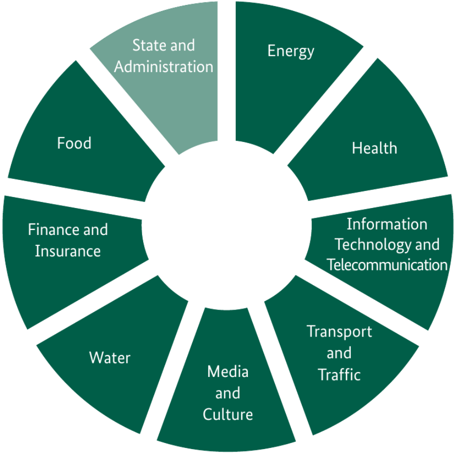
Information Technology vs. Operational Technology

vs.

Confidentiality Integrity Availability Privacy Authenticity

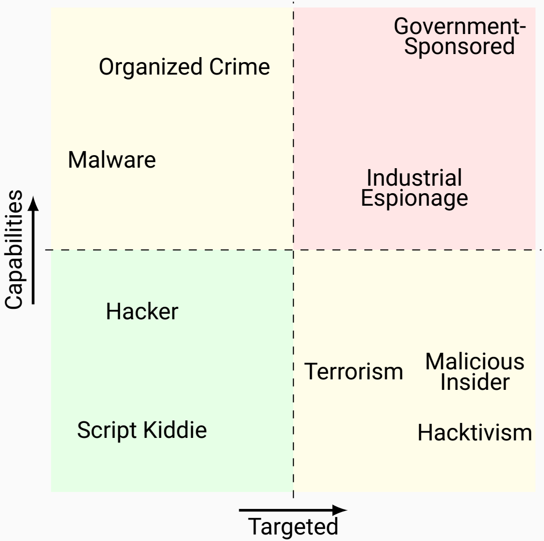
+Safety +Impact on environment and society

Critical Infrastructures



Federal Office for Civil Protection and Disaster Assistance, "Critical Infrastructures", URL: `https://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html`.

Threat Sources



Common IIoT Threats

- Abuse
- Denial of Service (DoS)
- Destruction
- Espionage
- Intellectual property theft
- Maloperation
- Man in the Middle (MitM)
- Ransomware
- Repudiation
- Spoofing

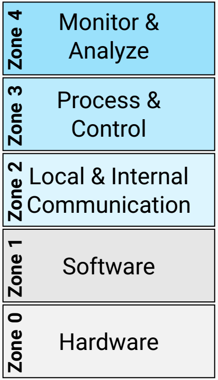
Common IIoT Vulnerabilities

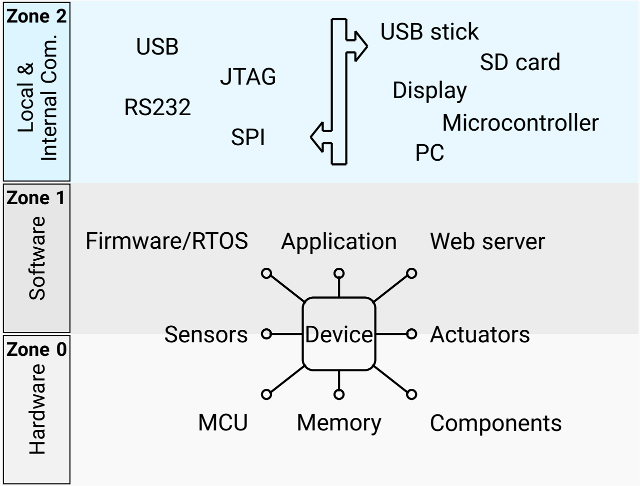
- Code execution
- Communication manipulation
- Design flaws and bugs
- Insecure and outdated components
- Memory manipulation
- Misconfiguration
- Physical manipulation
- Privilege escalation
- Repudiation
- Web-based vulnerabilities

Attack Vectors

Attack vectors:

- Device attacks

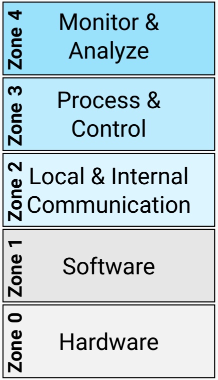




Attack Vectors

Attack vectors:

- Device attacks
- Application attacks
- Network attacks



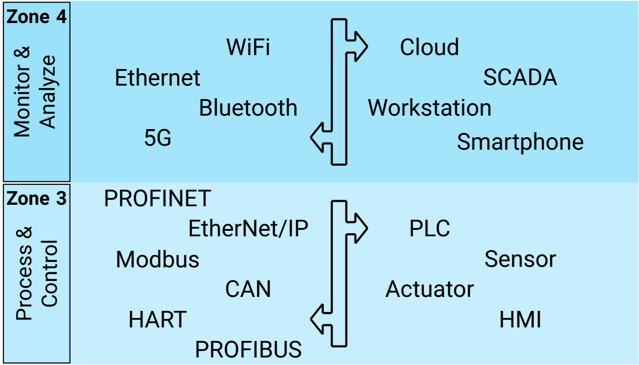
Zone 4 Monitor & Analyze

Zone 3 Process & Control

Zone 2 Local & Internal Communication

Zone 1 Software

Zone 0 Hardware



Zone 4 Monitor & Analyze

WiFi, Ethernet, Bluetooth, 5G

Cloud, SCADA, Workstation, Smartphone

Zone 3 Process & Control

PROFINET, EtherNet/IP, Modbus, CAN, HART, PROFIBUS

PLC, Sensor, Actuator, HMI

Recommended Procedure

1. Know your device
2. Creation of a network diagram
3. Identification and ranking of assets
4. Identification of threat sources
5. Identification of threats and vulnerabilities
6. Vulnerability and risk assessment

Conclusion

- Usage in critical infrastructures increases risks
- Additional threats through physical processes
- Additional vulnerabilities through insecure old technology

Thank You! Questions?

The project iSEC is funded by the Bavarian State Ministry for Economic Affairs, Regional Development and Energy within the framework of the Bavarian funding program for research and development “Information and Communication Technology”.