SPONSORED BY THE

Velektronik

Federal Ministry
of Education
and Research

Security with Chains of Trust

Challenges

- **Complex production processes** of electronic components from different manufacturers
- **Trust in manufacturers?**

Manufacturing Quality

Functionality

Authenticity

Trustworthiness of electronic components affected by

- Strained supply chain
- Increasing number of cyber-threat scenarios

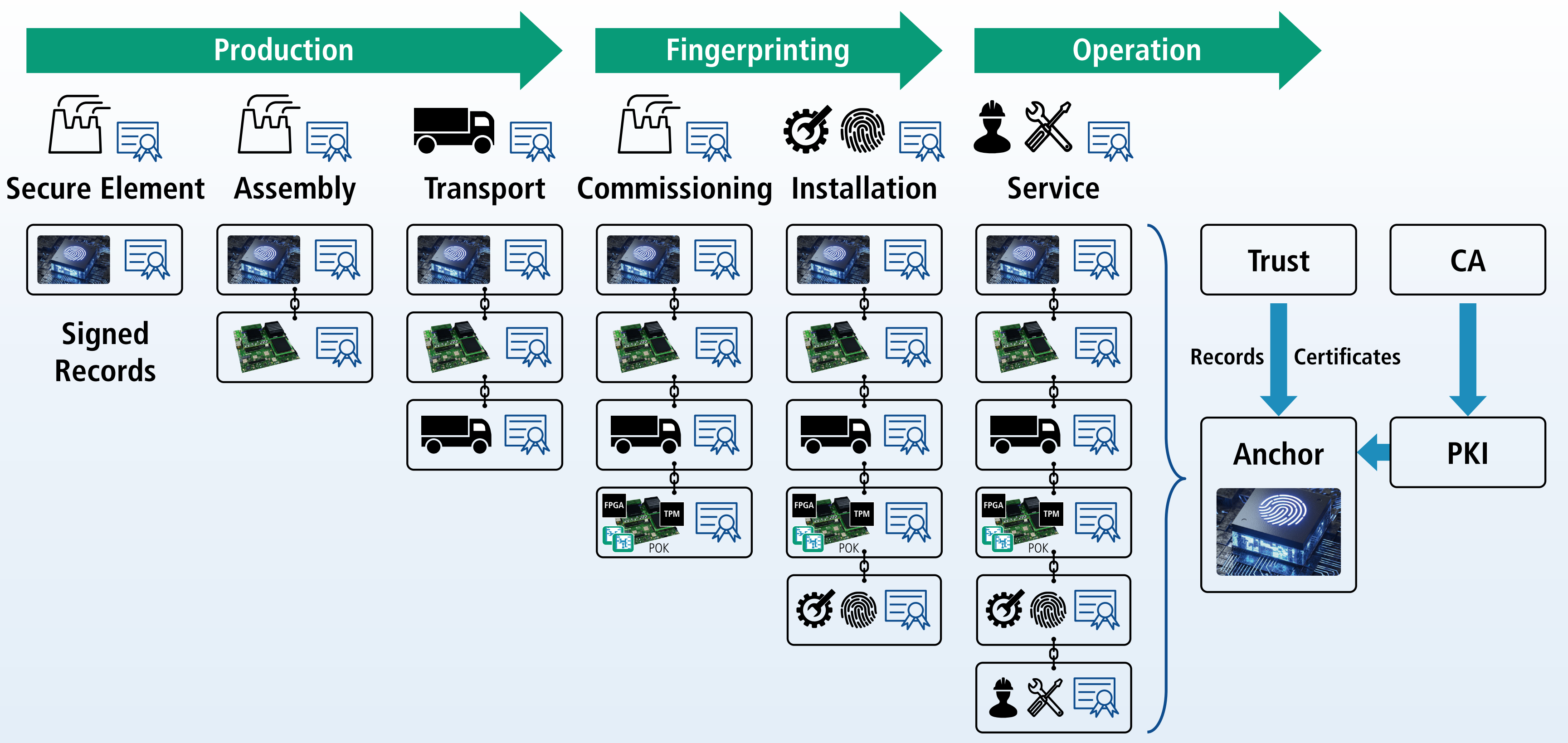
Chain of Trust (CoT)

- Recording **production steps, commissioning process, and hardware characteristics**
- Cryptographically secured chains (CoT)
- Safe storage in **Secure Element (SE)**

Goals

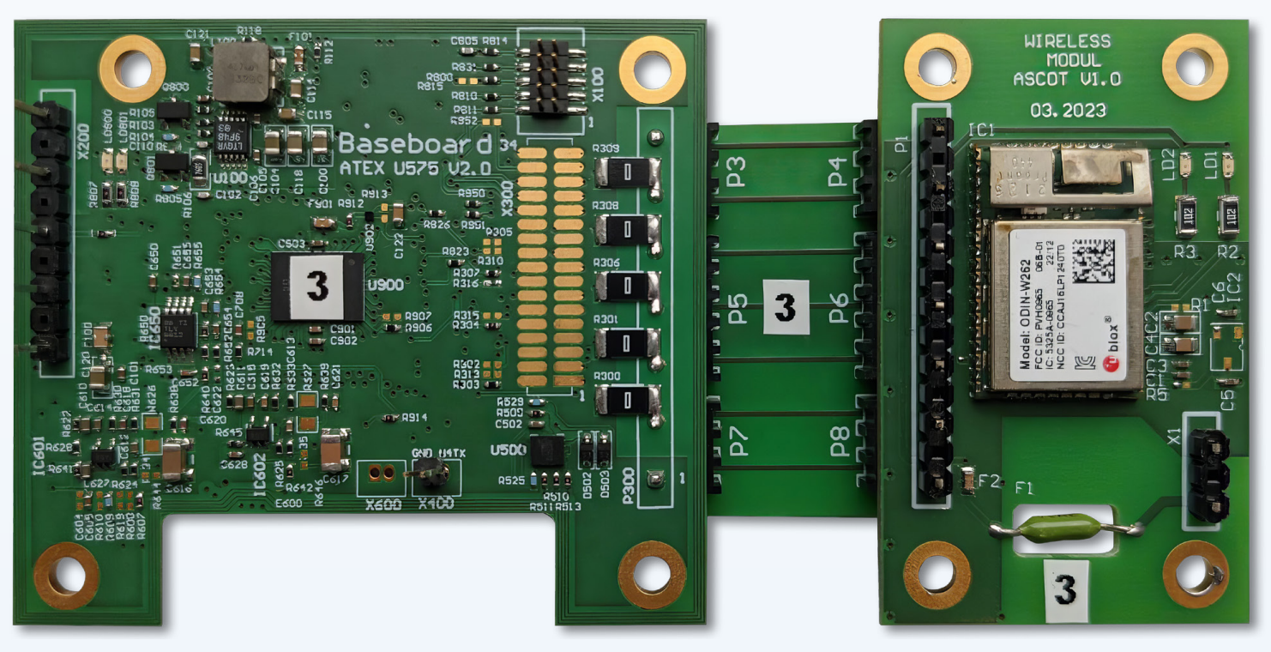
- Proof of integrity
- Remote attestation
- Component integrity assurance
- Continous verification of trustworthiness

Trusted Product Lifecycle Management



IoT Demonstrator

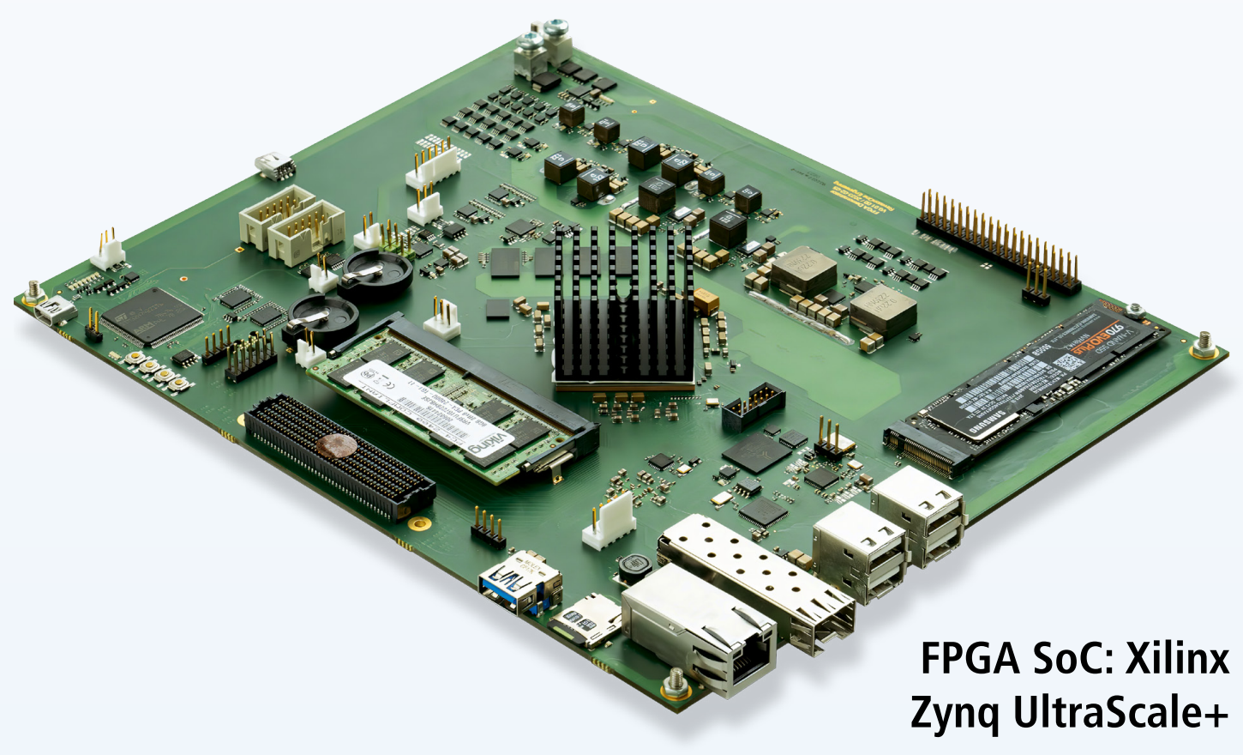
Industrial condition monitoring



Microcontroller: STM32U575 Cortex

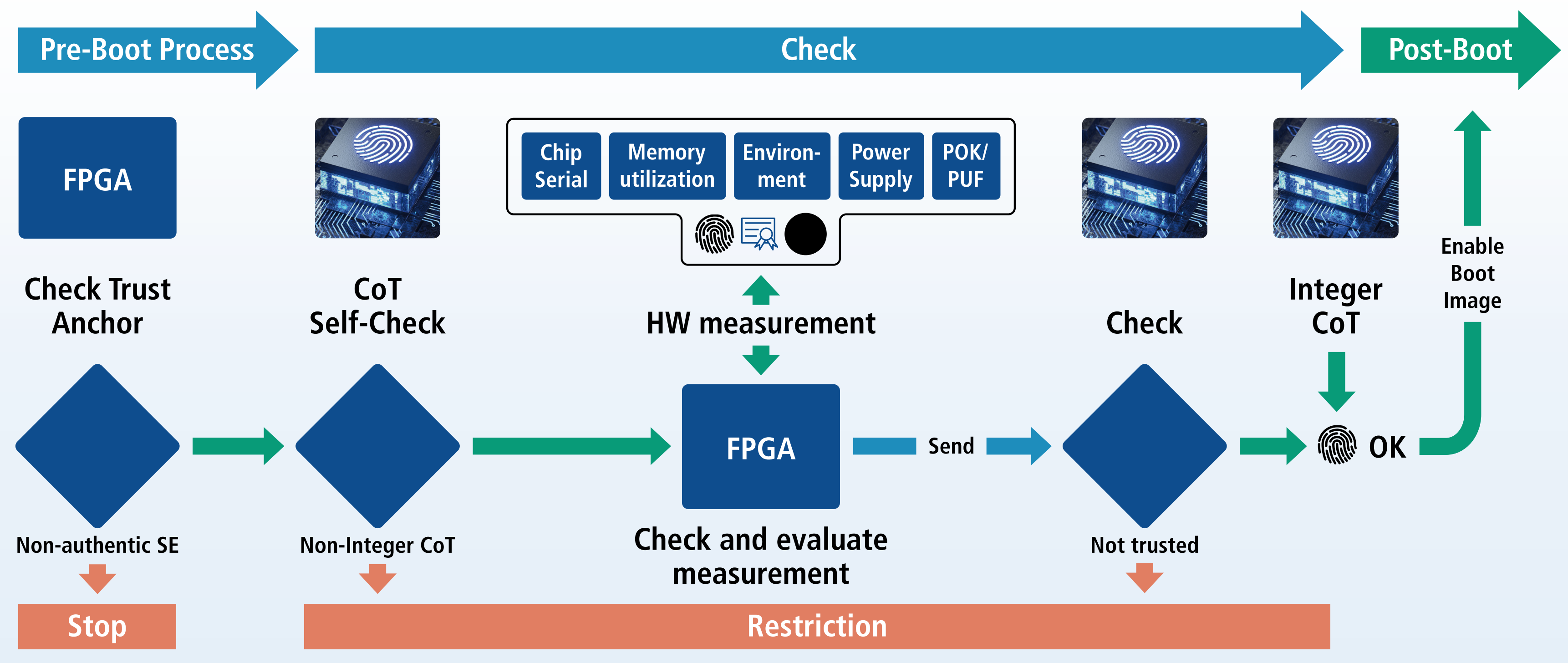
Edge Computing

Medical devices



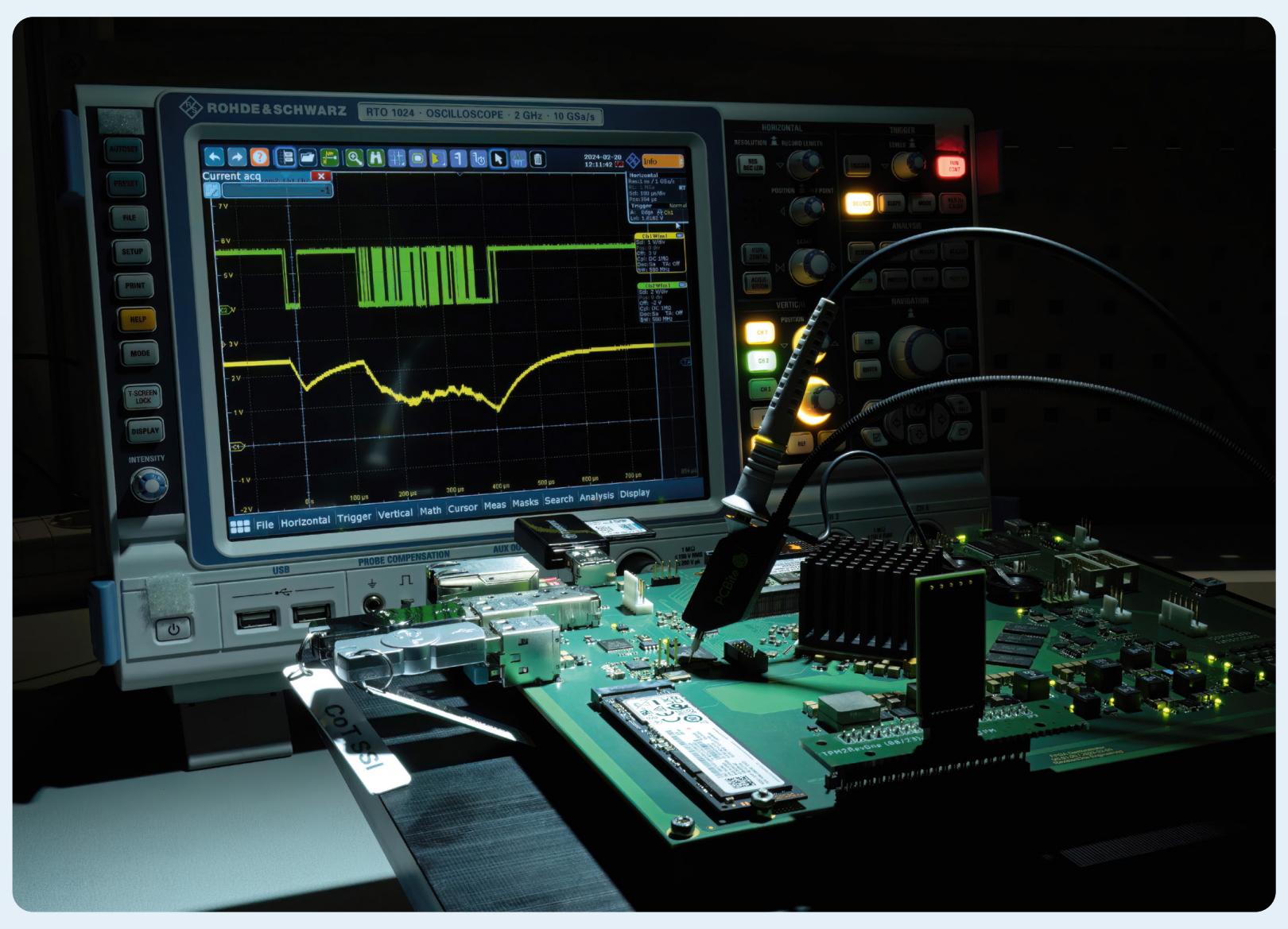
FPGA SoC: Xilinx Zynq UltraScale+

Trusted Boot



Hardware Features

- **Security Components**
  TPM, POK, WIBU-SE
- **Power Supply Monitoring**
  200 KSPS @16-bit: voltages and currents
  65 MSPS @18 bit: bus analysis
- **System Monitoring**

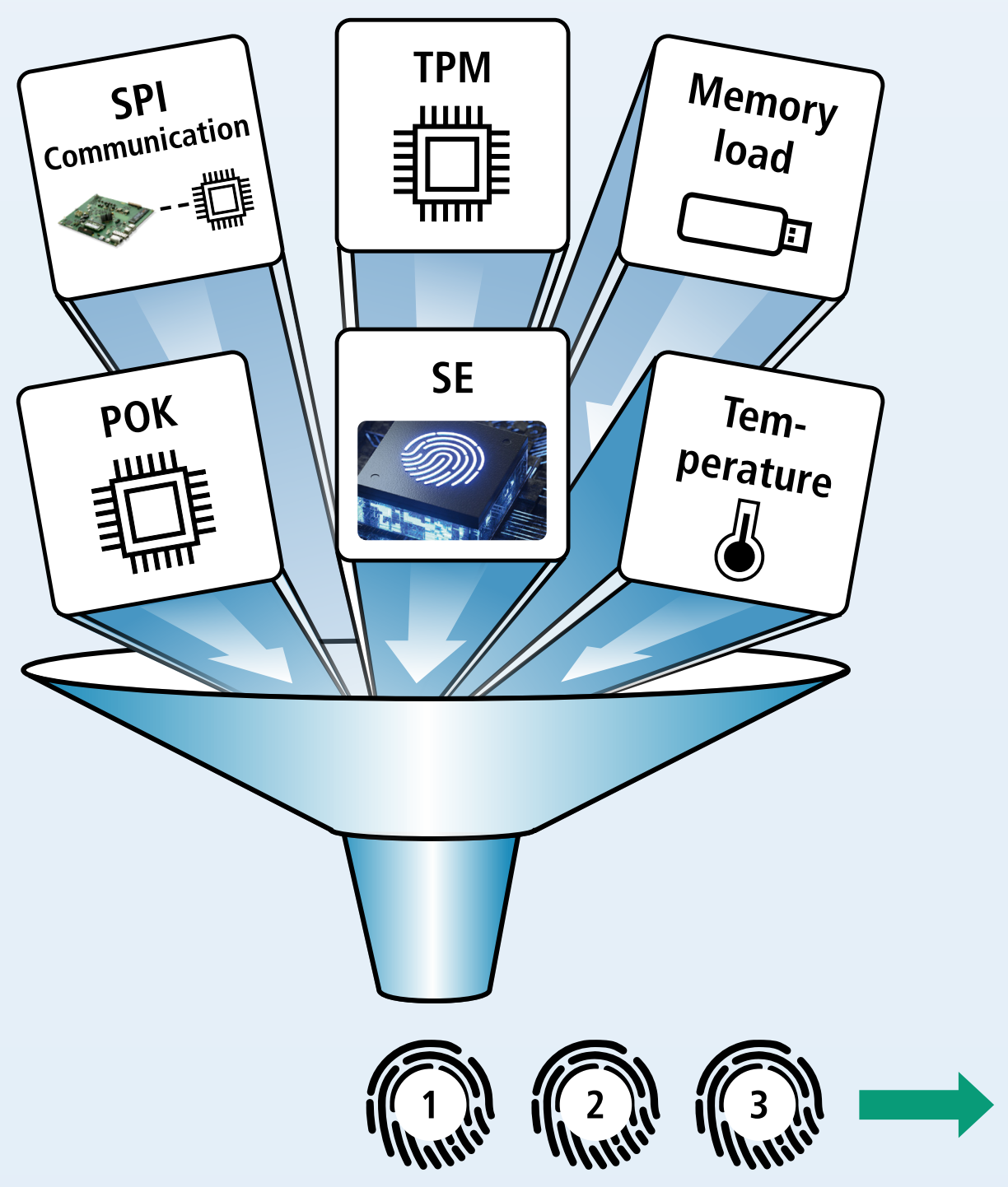


Fingerprinting

Uniquely identify assembly groups to **detect manipulations, anomalies, and counterfeiting**

Approaches

- Stochastical Analysis
- Machine Learning
- Fuzzy Extractor



Project Information

Volume
EUR 4,71 million

Project Duration
03/2021 - 02/2024 (extended until 12/2024)

Call
Trustworthy Electronics (ZEUS)

WIBU SYSTEMS | Infineon | SIEMENS | UNIVERSITÄT BIELEFELD | KIT Karlsruher Institut für Technologie | Fraunhofer SIT

Contact:
Ralf Fust | ralf.fust@wibu.com | www.ascot-trust.info