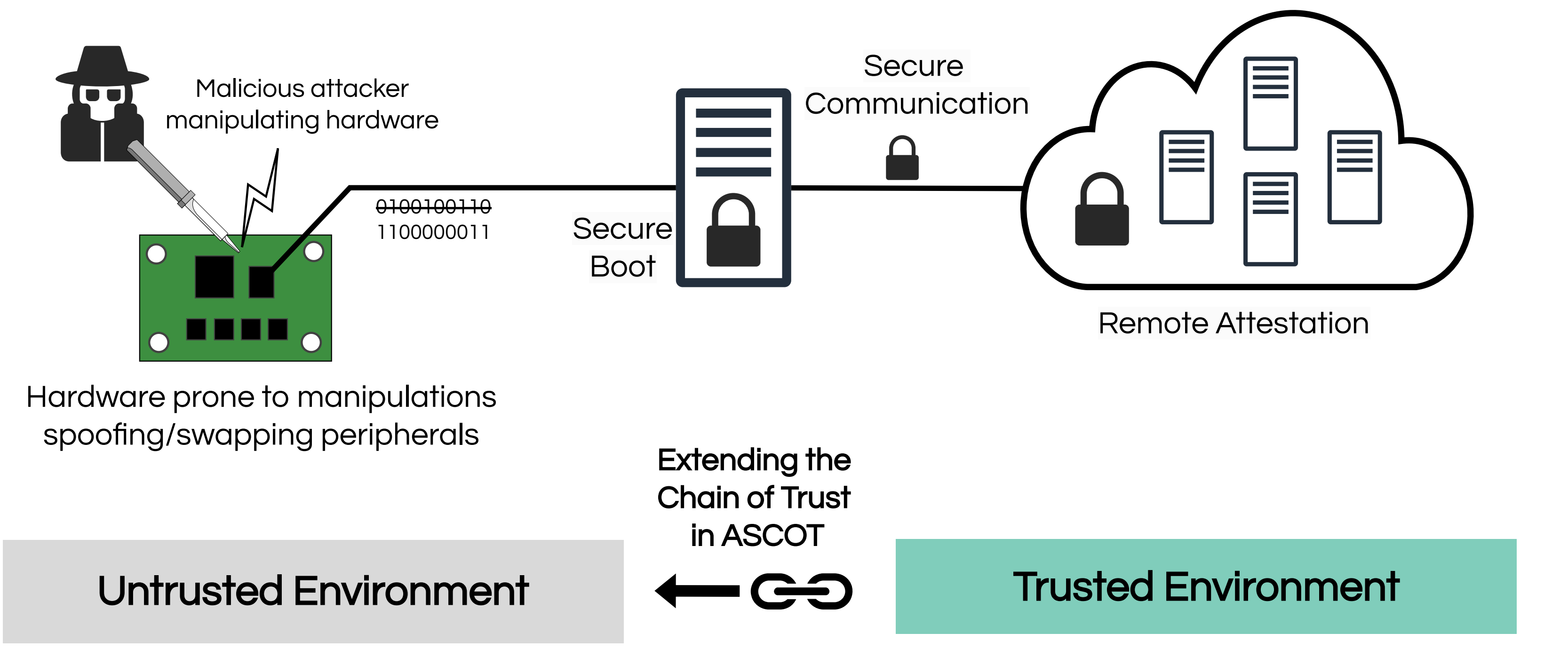
Hardware Integrity Validation for Trustworthy Computing in Embedded Systems

Velektronik
Bundesministerium für Bildung und Forschung
VE-ASCOT
03/2021-12/2024

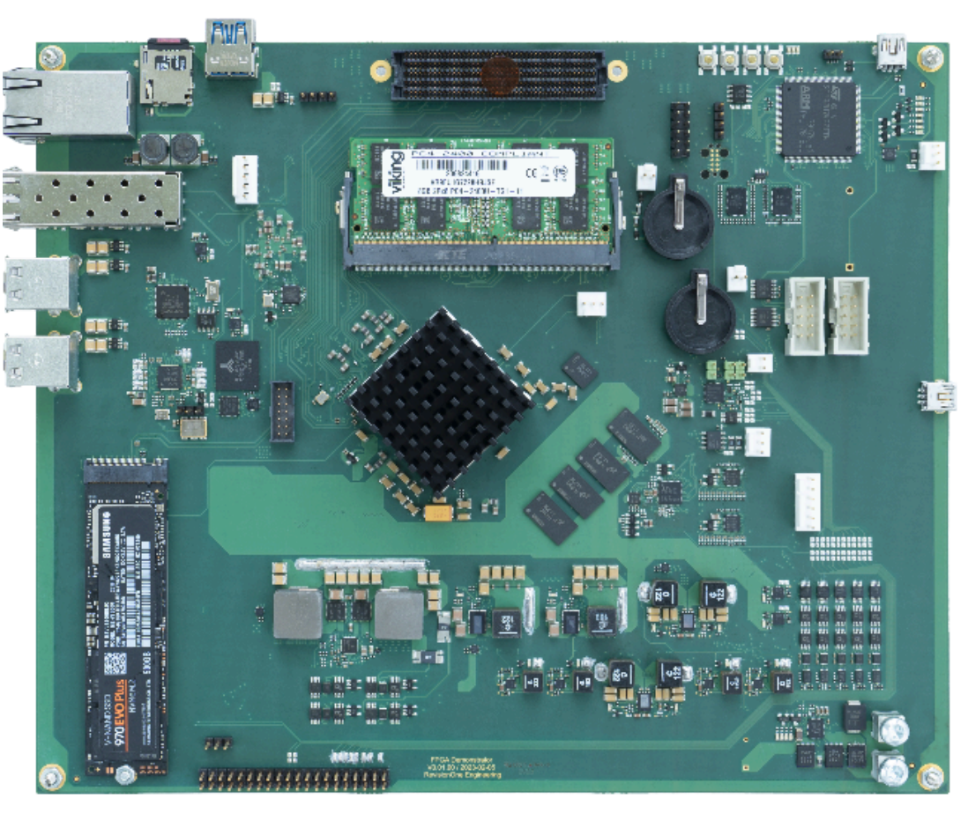
Motivation

- Critical appliances, e.g. in medical or public transportation require a high level of system integrity
- Mechanical hardware tamper detection is insufficient
- Goal: Create an integrated platform to detect unqualified repairs or reverse engineering/ spoofing attacks at run-time

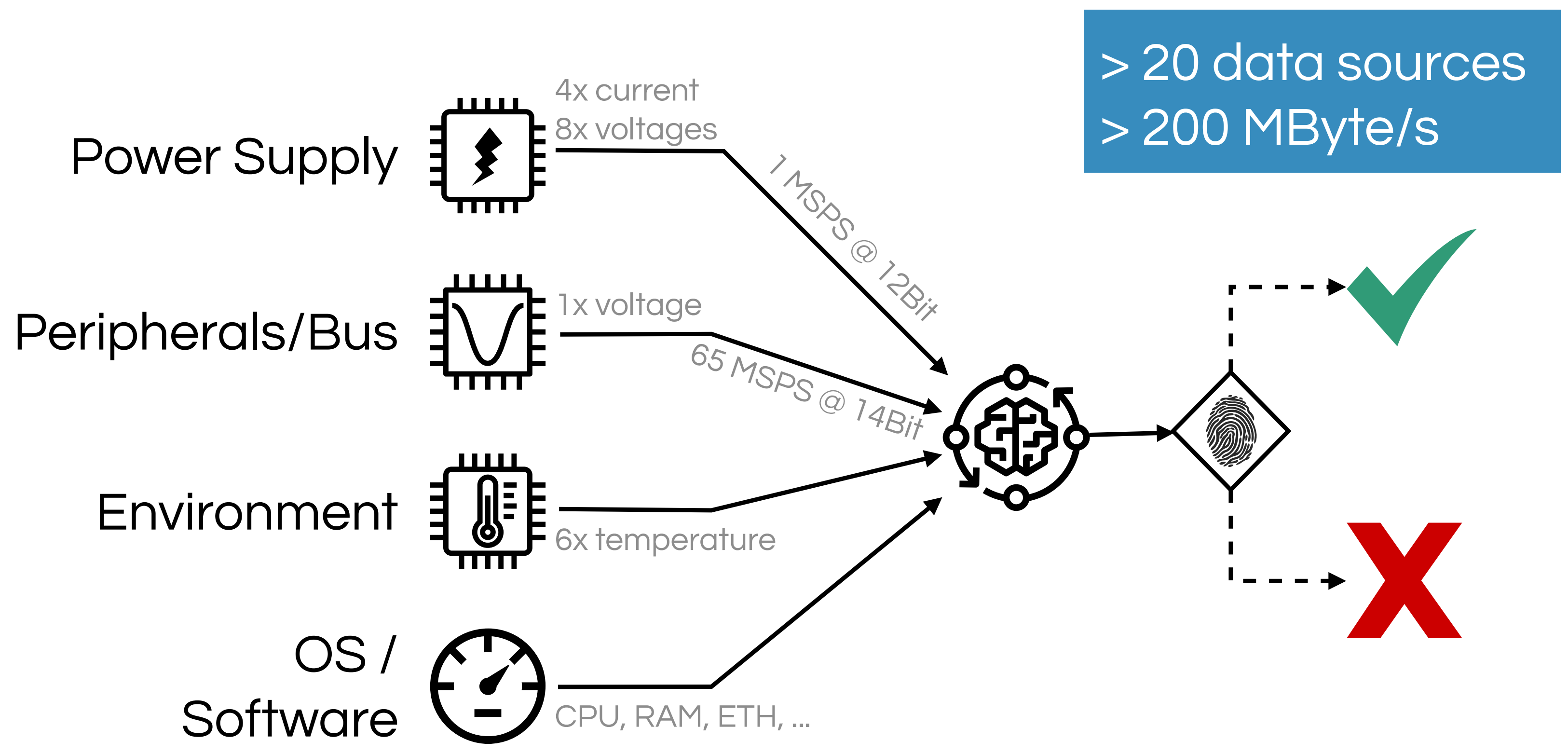

Malicious attacker manipulating hardware
~~0100100110~~
1100000011
Secure Boot
Secure Communication
Remote Attestation
Hardware prone to manipulations spoofing/swapping peripherals
Extending the Chain of Trust in ASCOT
Untrusted Environment
Trusted Environment

Hardware Platform

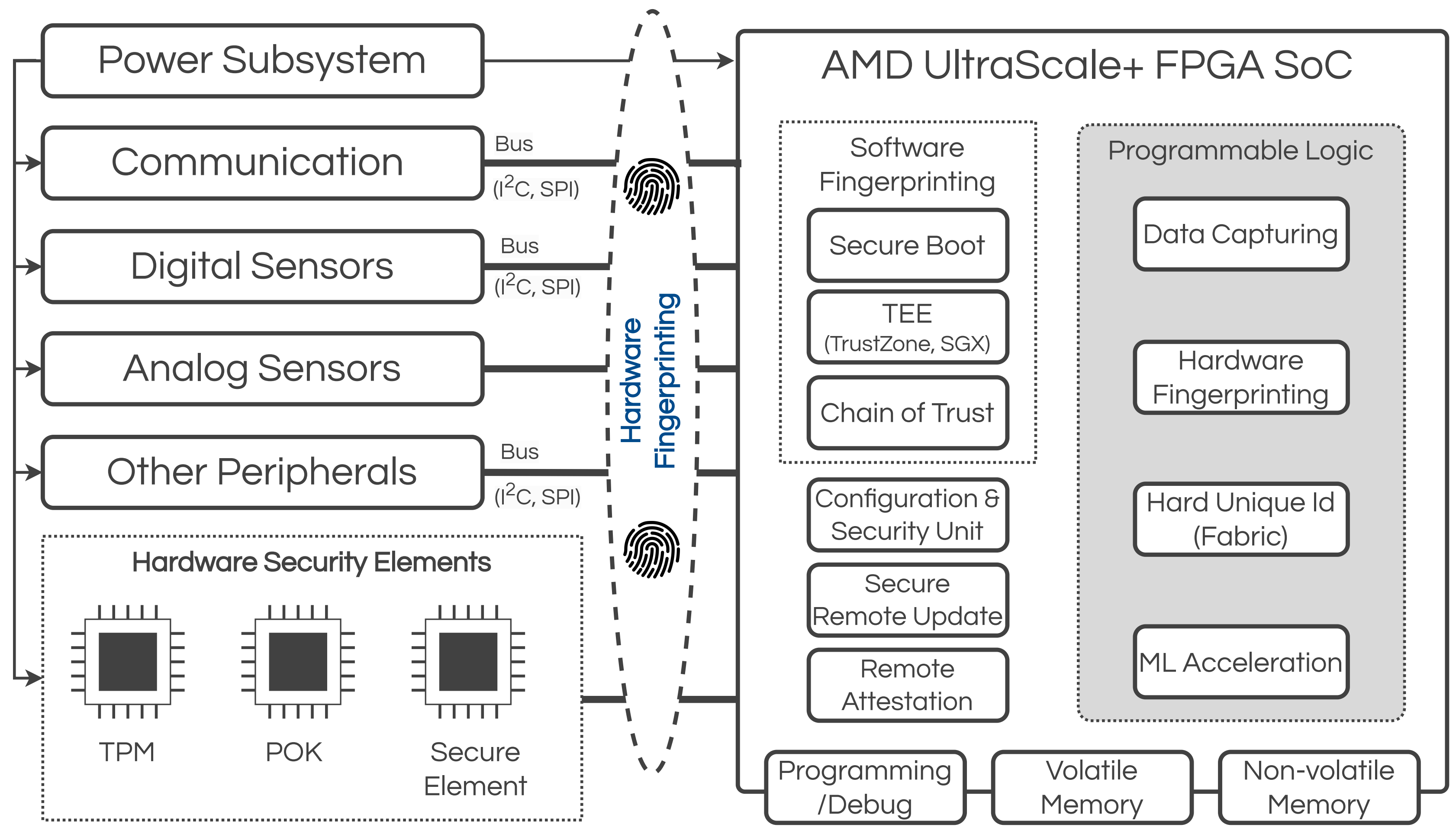
- Typical edge computing hardware based on high performance FPGA-SoC technology (AMD UltraScale+)
- Integrated security components (TPM, Secure Element and POK)
- Sensors for hardware monitoring:



> 20 data sources
> 200 MByte/s

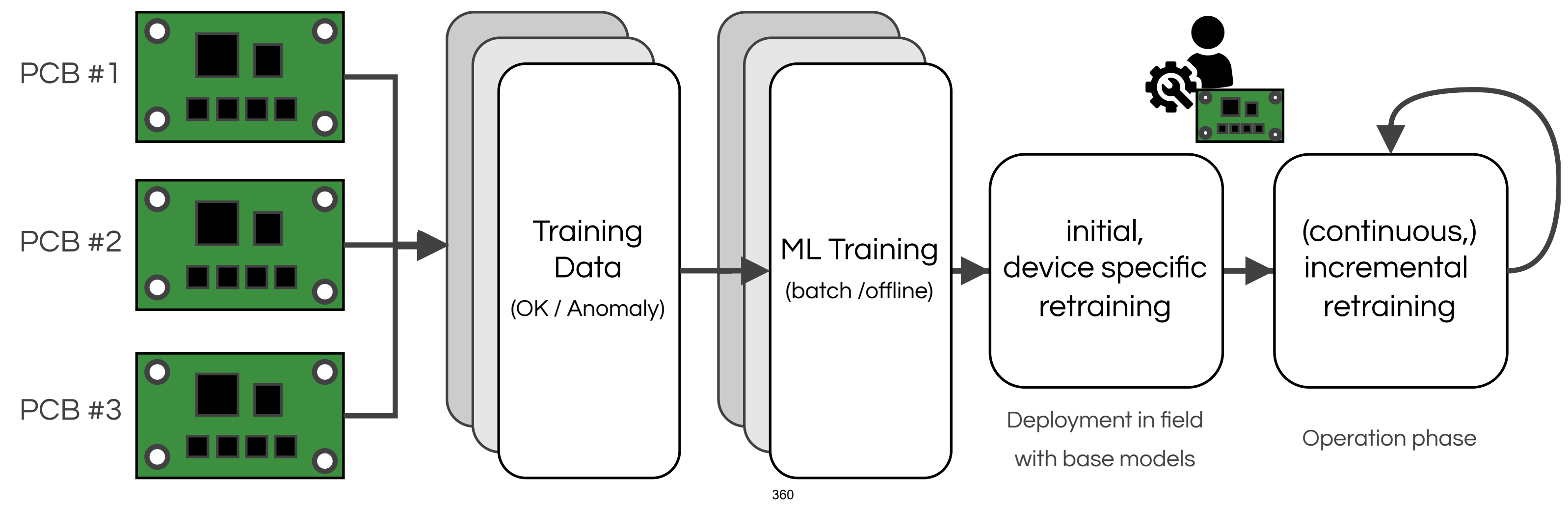


System Architecture



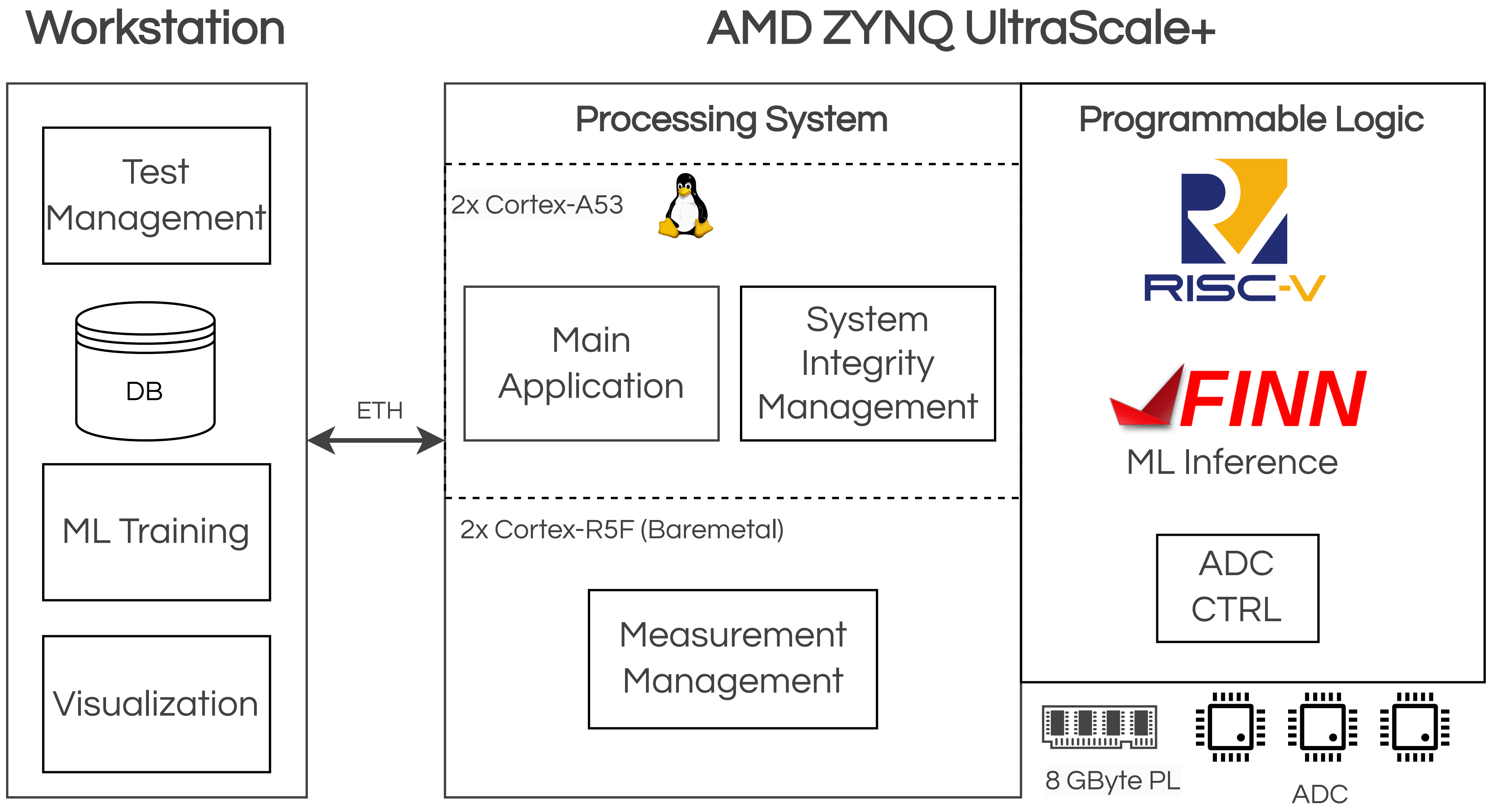
Manipulation Detection

- Hardware manipulations are mainly irreversible
- Only few data sets with manipulations recordable
  ➔ Train Auto Encoder for anomaly detection based on unmanipulated data
- Impact of aging effects yet unclear
  ➔ Re-training in field operation as feasible extension


PCB #1
PCB #2
PCB #3
Training Data
(OK / Anomaly)
ML Training
(batch /offline)
initial, device specific retraining
(continuous,) incremental retraining
Deployment in field with base models
Operation phase
360

Data Aquisition and Processing

- Real-time data aquisition with ~200 Mbyte/s
- Automated data aquisition: >10k of different time series are required as training data for machine learning
- Target platform is too constrained for in-system training
- Different sample rates of sensors requires pre-processing
- Minimize influence of measurements and processing on actual appliance
- Support for integrity validation at pre-boot, idle and dynamic system states



Contact

Christian Stollenwerk
Bielefeld University

Martin Kaiser
Bielefeld University

Universität Bielefeld
Siemens
KIT Karlsruher Institut für Technologie
RevisionOne Engineering GmbH
WIBU Systems
Fraunhofer SIT
Infineon
Schölly Excellence Inside

www.ascot-trust.info