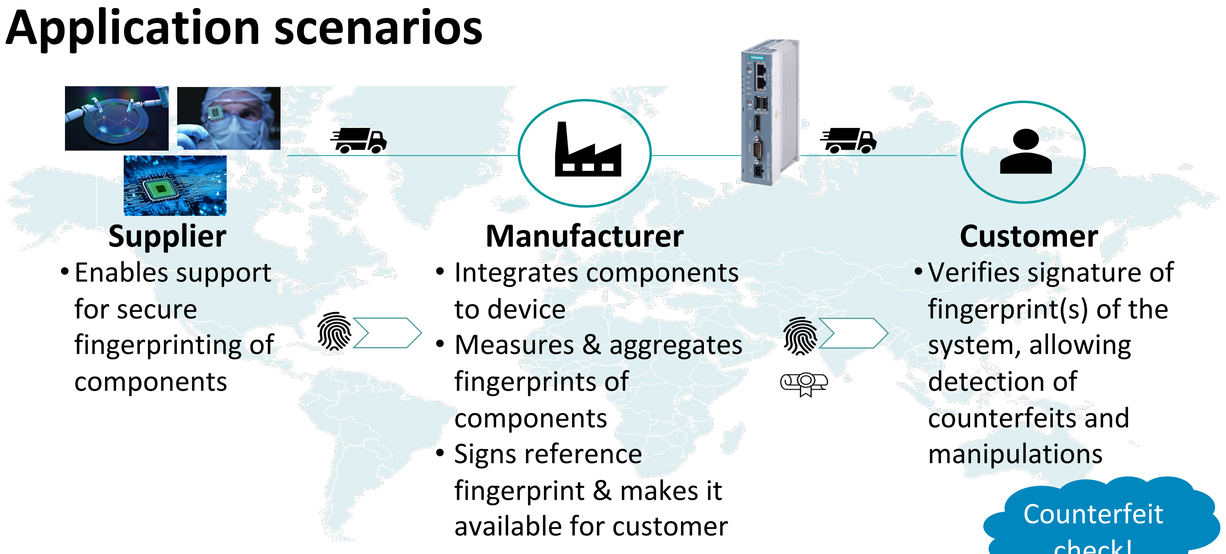
# VE-FIDES: Designing Trustworthy Supply Chains Using Innovative Fingerprinting Implementations

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

## Application scenarios



**Supplier**
- Enables support for secure fingerprinting of components

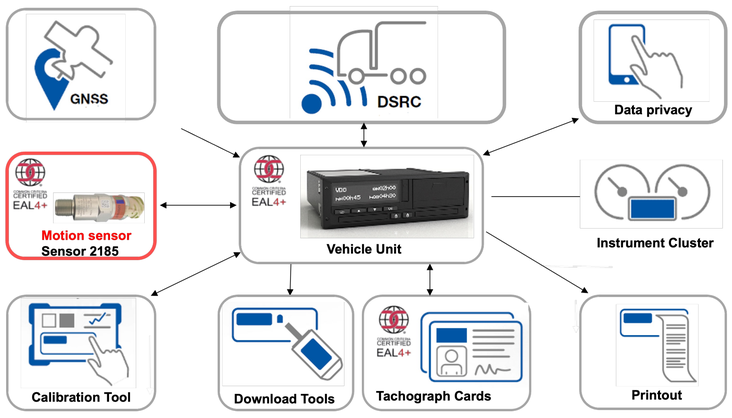
**Manufacturer**
- Integrates components to device
- Measures & aggregates fingerprints of components
- Signs reference fingerprint & makes it available for customer

**Customer**
- Verifies signature of fingerprint(s) of the system, allowing detection of counterfeits and manipulations

Counterfeit check!

- Demonstrating hardware component integrity check of an industrial device

### Overview digital tachograph system – Continental



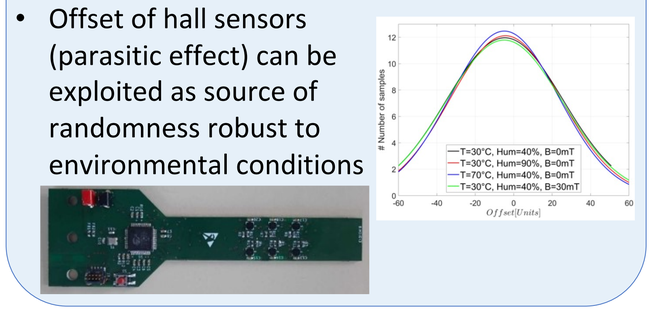

- Enhanced fingerprinting security solution within motion sensor possible?

## Fingerprinting from physical properties

- Researching novel methods at circuit board level for system authenticity and detection of unauthorized chip/PCB alterations
- Monitoring externally measurable parameters to recognize alterations in circuitry or components
- Utilizing existing chips or ASICs specifically designed for identifying changes to circuit board components and electronic functionalities

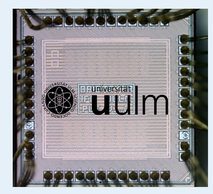
### On chip fingerprinting – TUM LSE

- Offset of hall sensors (parasitic effect) can be exploited as source of randomness robust to environmental conditions




### On chip fingerprinting – University of Ulm

- Development of exemplary ASICs for trustworthy fingerprint generation
- *Eye-Opening-Arbiter* PUF architecture to generate unique chip ID
- Exceptional reliability (BER<2.7e-7) shown by measurements over wide temperature, supply voltage and ageing range

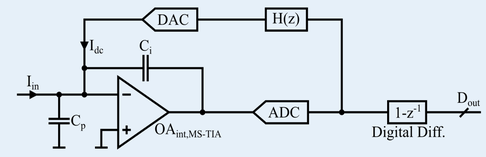



### On chip fingerprinting – Infineon

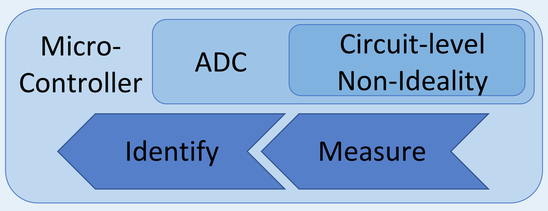
- Arbiter-based architectures – pure logic
- Test chip developed and measured over broad temperature and voltage ranges
- Error correction code able to compensate instabilities over environmental variations and aging


### Printed circuit boards trustworthiness

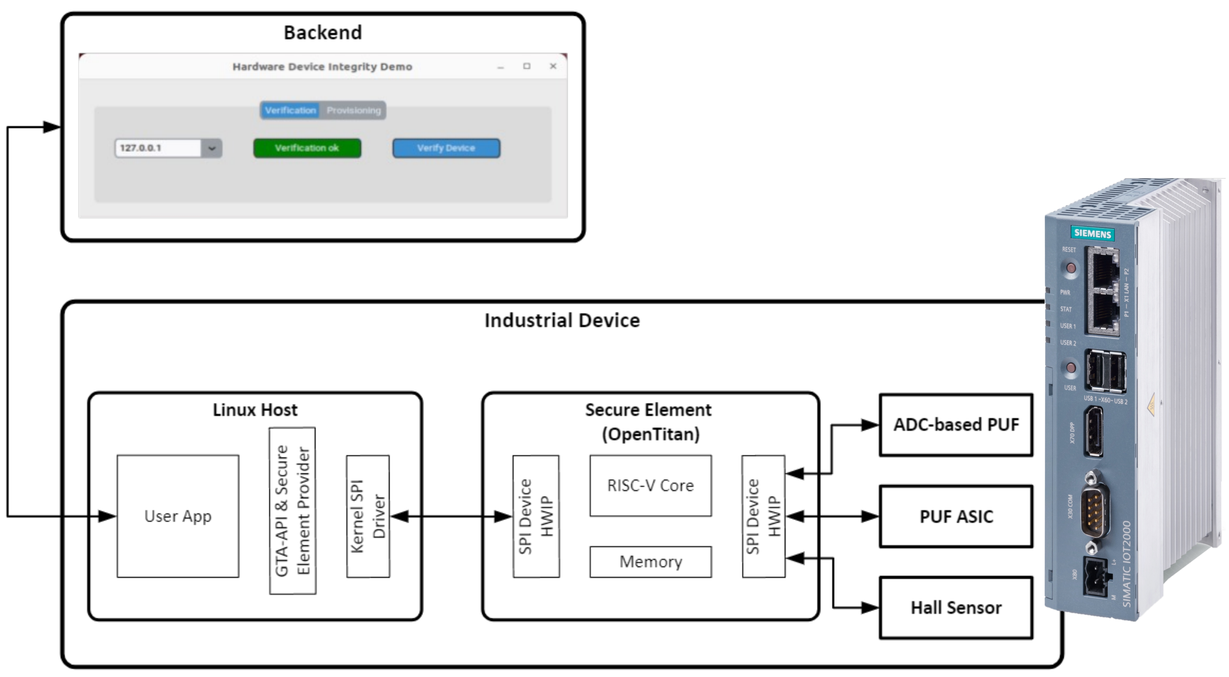
- Implicit & Explicit PCB identification
- Novel TIA-based fingerprint measurement system




- Microcontroller self-identification by utilizing ADC-based fingerprinting techniques
- Sensor ID by TUM
- PCB characterization by Bischoff E.




## Demonstrator – Fingerprinting for trustworthy electronic system

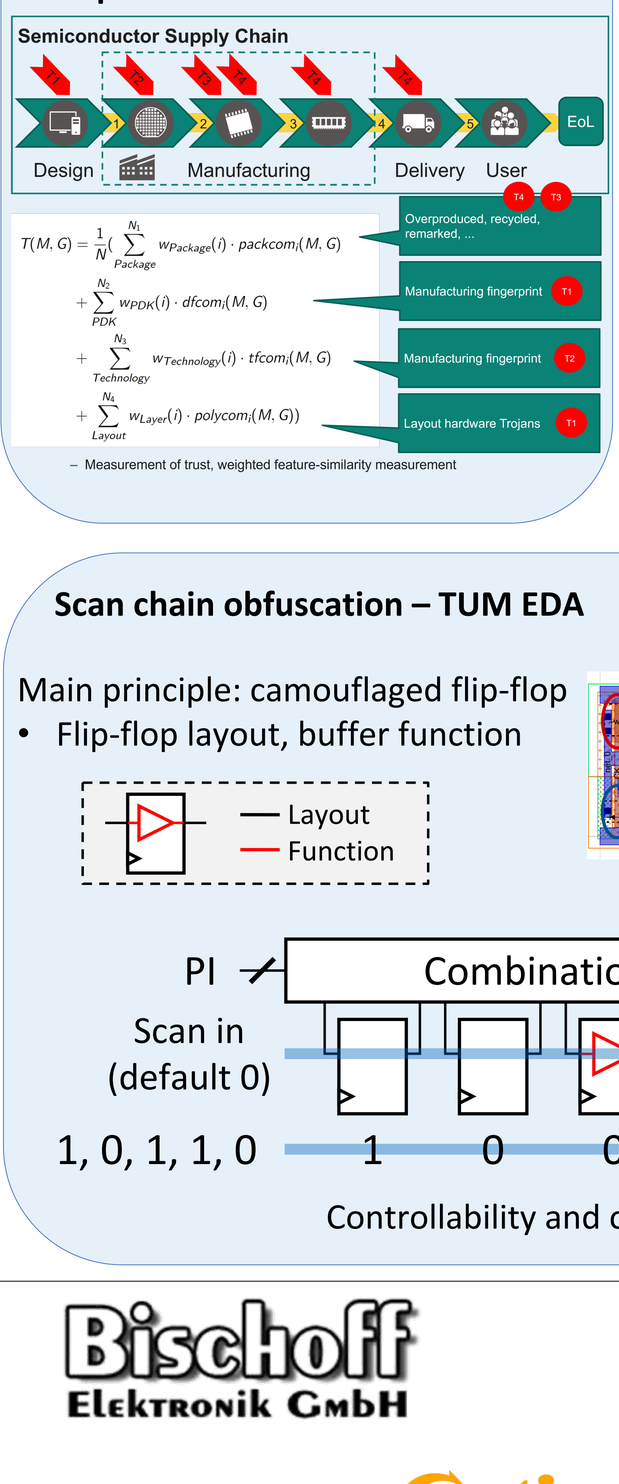



**Objective**:
The demonstrator (with contributions by all partners and lead by Fraunhofer AISEC) will illustrate the verification of integrity and authenticity of device's hardware components in the field and along the supply chain

**Approach**:
Device components having unique fingerprints, derived from physical properties, are verified by measuring these fingerprints and comparing them with reference fingerprints provided by the device manufacturer. For a developer-friendly verification GTA API is used.

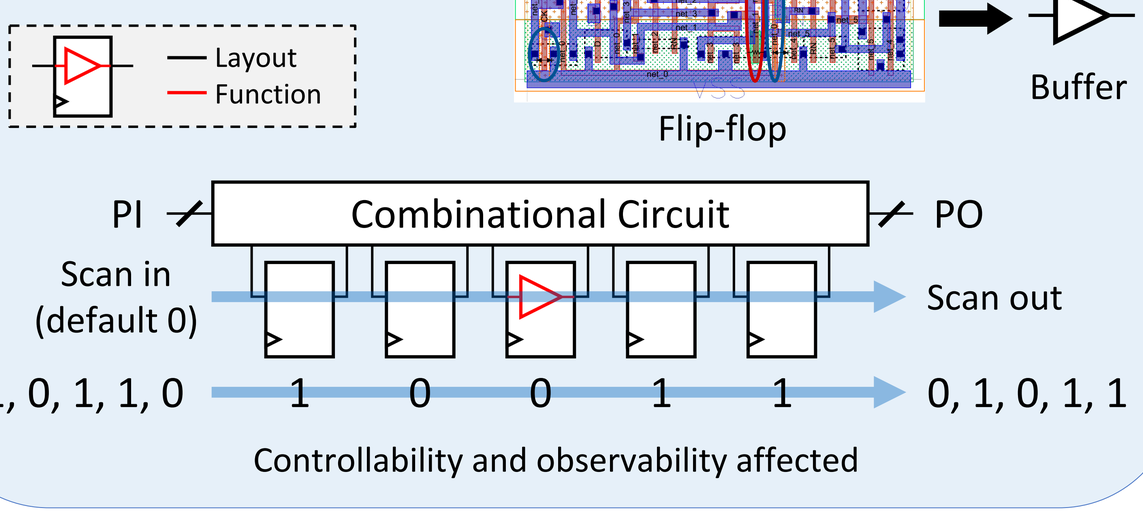
## Protection with reverse engineering methods

### Trust assessment through physical inspection – Infineon




### Scan chain obfuscation – TUM EDA

Main principle: camouflaged flip-flop
- Flip-flop layout, buffer function




## Developer-friendly hardware integrity check using fingerprinting with RISC-V based secure element

- Standardized **Generic Trust Anchor API (GTA API)**:
  - facilitates efficient integration of crypto-based security.
  - provides mechanisms to establish device trust.
  - abstracts different trust anchor technologies.
  - enables crypto agility.
  - increases flexibility, e.g., to address regional crypto requirements.
- In **VE-FIDES**, Siemens developed and implemented a GTA API profile for verifying the integrity of hardware components integrated in an attached system.
- In the attached system, a secure element handles all security functionalities, e.g., cryptographic operations or fingerprinting.
- In **VE-FIDES**, TUM SEC implemented an OpenTitan-based secure element and researched methods to derive a PUF-based system fingerprint. The system may consist of many different components each with individual capabilities regarding performance and extractable PUF entropy.