

Dr.-Ing. Matthias Hiller

Challenges and technologies towards secure embedded systems and trusted electronics

SEMICON EUROPA, November 15, 2023, Munich

partly funded by



Bundesministerium
für Bildung
und Forschung

Bayerisches Staatsministerium für
Wirtschaft, Landesentwicklung und Energie





**Who of you trusts the electronic devices
you are using?**

Definition: trusted electronics

Hardware must

1. meet high levels of quality and reliability

Reliable operation in the field over its full lifetime.

2. comply to a known and complete specification

Functionality cannot be altered from the specification.

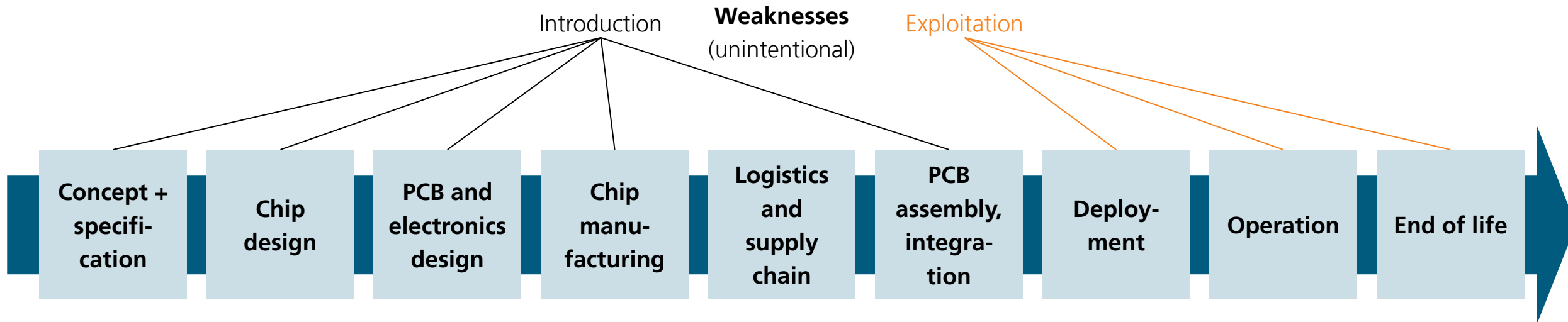
3. be sufficiently hardened against attacks

Mechanisms to ensure security and avoid vulnerabilities.

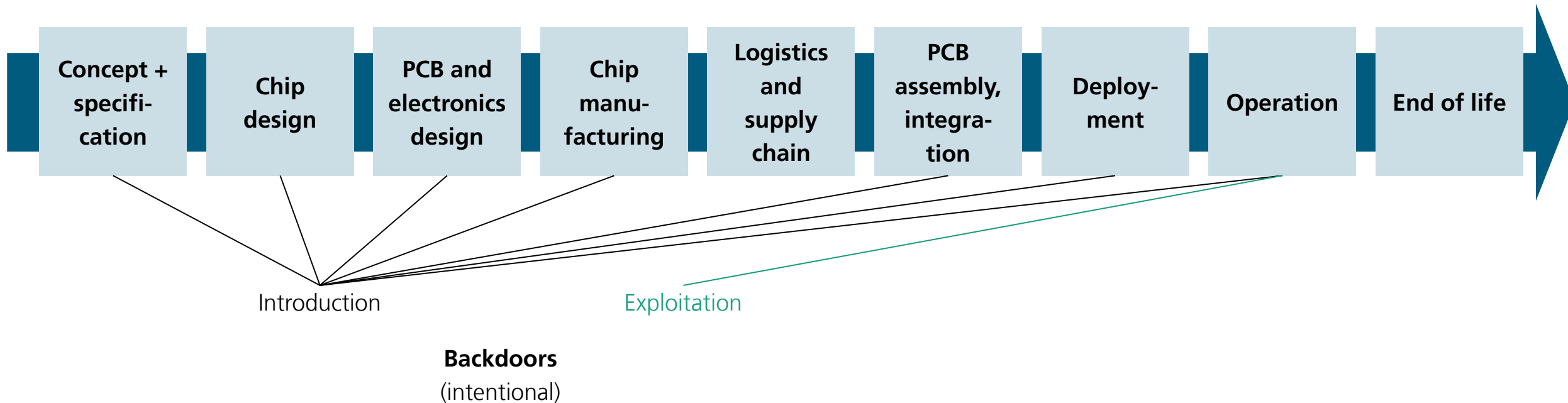
Electronics value chain



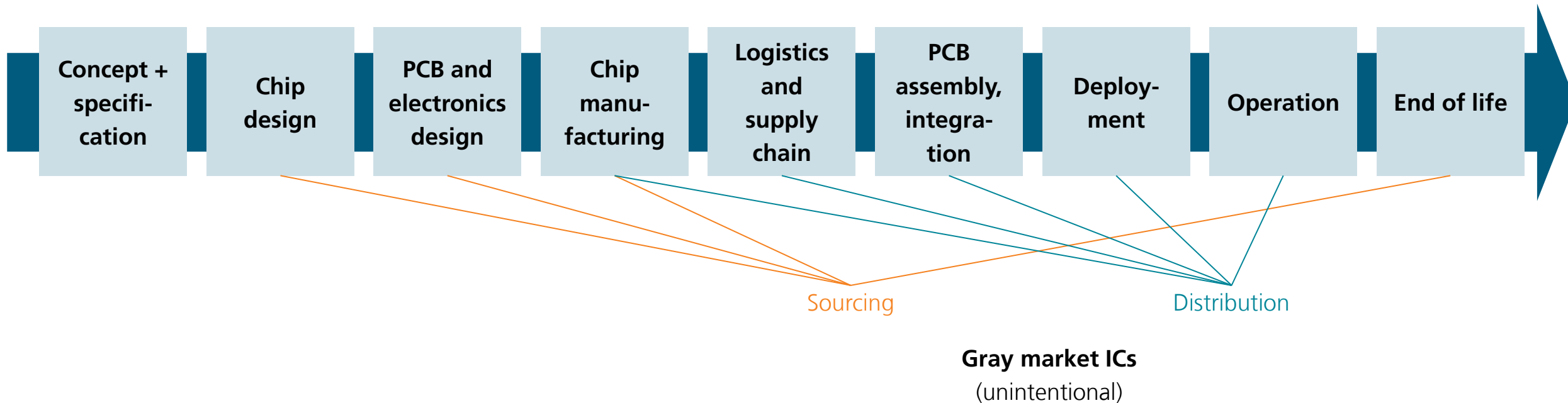
Vulnerabilities along the value chain: Weaknesses



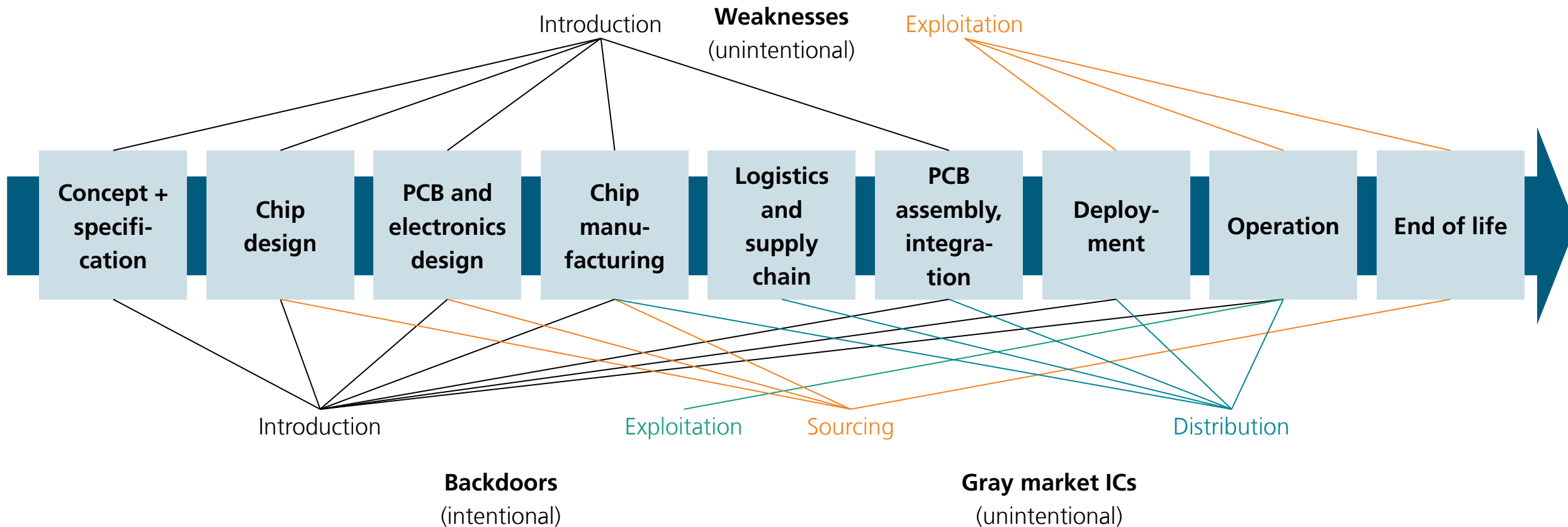
Vulnerabilities along the value chain: Backdoors



Vulnerabilities along the value chain: Gray market ICs



Vulnerabilities along the value chain





Examples for technologies towards secure
embedded systems and trusted electronics

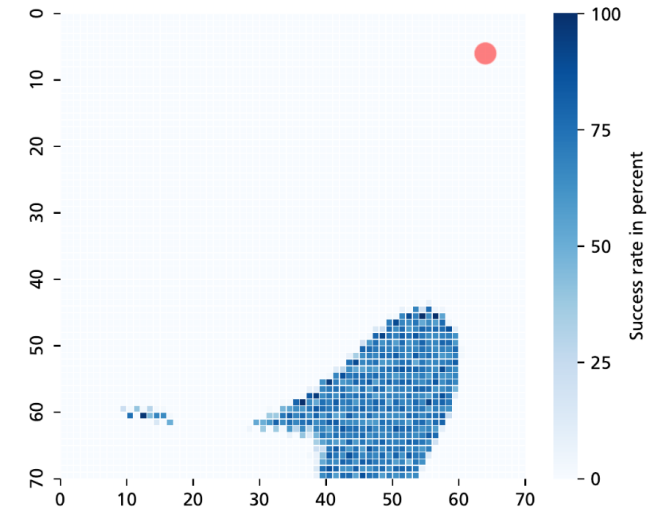
Practical security analysis

Side-channel analysis

- Power, EM, optical
- Cache, memory

Fault analysis

- Power and clock glitching
- EM
- Laser fault injection



Case study:

- Suppression of flash erases

BSI, "A Study on Hardware Attacks against Microcontrollers.", 2023.

Tamper protection for secure operation and supply chain security

Protect the supply chain and the data on the device

Physical unclonable functions and hardware fingerprinting

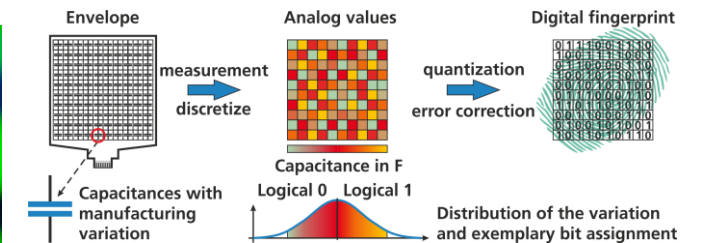
Possible features across the entire manufacturing chain

- Chip-level
- Package-level
- System-level

PUF-based tamper protection foil



© Fraunhofer EMFT / Bernd Müller.



Immler, et al. "B-TREPID: Batteryless tamper-resistant envelope with a PUF and integrity detection." HOST, 2018.

Conclusion and outlook

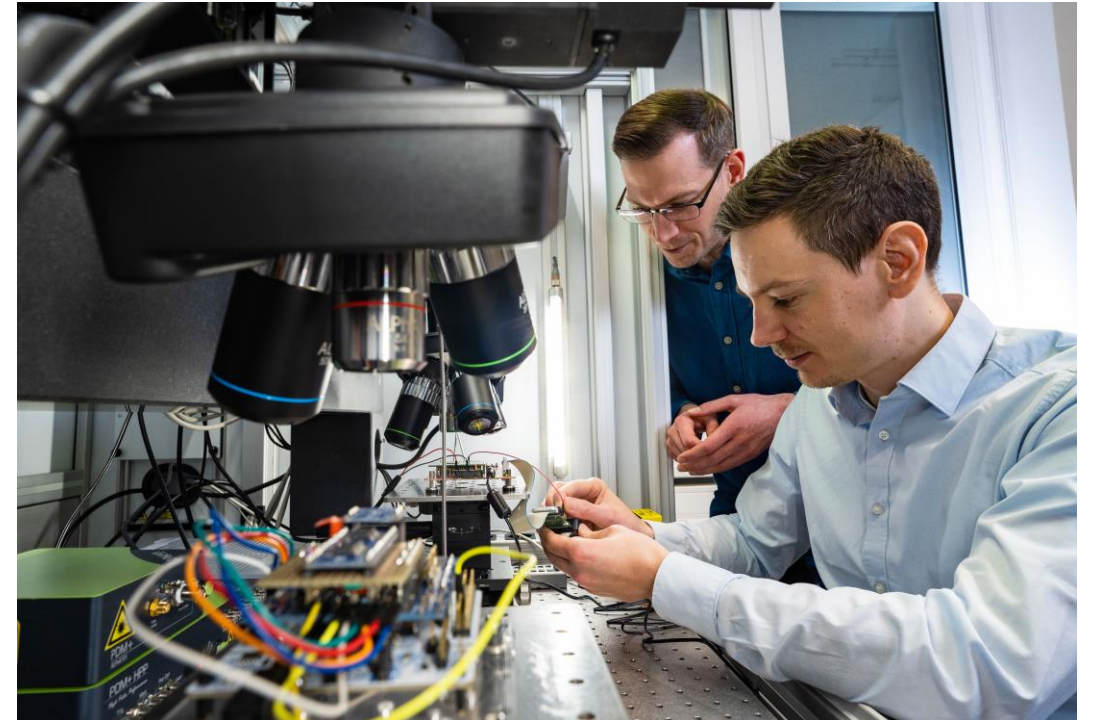
Complex problem to protect

- devices against a wide range of threats
- loose international supply chains

Technological

- solutions, tools and methods towards more trusted electronics

Major progress can only be achieved by joint effort of industry, research community, government, and corresponding research funding



Contact Information

Dr.-Ing. Matthias Hiller
Head of Department Hardware Security
Phone: +49 89 3229986-162
matthias.hiller@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security AISEC
Lichtenbergstraße 11
85748 Garching (near Munich)
Germany
www.aisec.fraunhofer.de



Fraunhofer Institute for Applied
and Integrated Security AISEC