Johanna Baehr

27th June 2024, RISC-V Summit, Munich

RISC-V and Trusted Electronics: a match made in heaven?

RISC-V and Hardware Security

Secure Boot

Trusted Execution Environment

Countermeasures against Side-channel Attacks

Crypto Extensions

Fault Injection Protections

Memory Protection

Formal Verification Support

Hardware Random Number Generator

Secure Remote Attestation

… and many more!

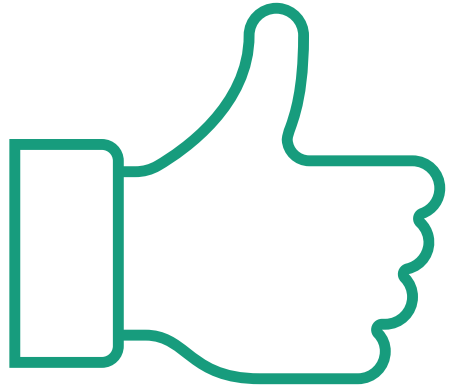
Hardware Security < **Trusted Electronics** < Technological Sovereignty

Trusted Electronics: What does it mean for a Component?

no hardware Trojans, backdoors, or hidden functions

comes from a trustworthy supply chain

measures to protect against unauthorized changes



Minimized risk of unspecified behavior

Properties of Trusted Electronics

Overview

1. The hardware must meet **high levels of quality and reliability**.

Reliable operation in the field should be guaranteed over its full lifetime.

2. The hardware must comply to a **known and complete specification**.

Functionality should not deviate from the specification.

3. The hardware must be sufficiently **hardened against attacks.**

Mechanisms to ensure security and avoid vulnerabilities should be in place.

Heyzsl, Johann, et al. "Referenzpapier Vertrauenswürdige Elektronik." 2022.

Properties of Trusted Electronics

Quality and Reliability

1. The hardware must meet **high levels of quality and reliability**.

Reliable operation in the field should be guaranteed over its full lifetime.

1. **Verifiability:** open-source allows for verification by the community, many eyes principle
2. **Speed:** community efforts, peer reviews and collaborative testing (e.g. shared testing resources) allows for fast verification
3. **Reduced Complexity:** ability to customize and minimize the ISA reduces complexity
4. **Innovation & Competition**: Open ISA creates innovation and many new products, leading to high-quality

Properties of Trusted Electronics

Quality and Reliability: Challenges

1. The hardware must meet **high levels of quality and reliability**.

Reliable operation in the field should be guaranteed over its full lifetime.

1. Technical maturity of open-source hardware
2. Varying implementation standards by different vendors might affect uniformity in quality
3. Availability of software ecosystem
4. Ensuring (long-term) support

Properties of Trusted Electronics

Specification

2. The hardware must comply to a **known and complete specification**.

Functionality should not deviate from the specification.

1. **Open-Source:** allows for verification, vs closed source designs
2. **Documented:** ISA is well-documented, allowing for precise and verifiable compliance to specifications
3. **(Formal) Verifiability:** formal verification methods can be employed
4. **Governing Body:** RISC-V Foundation maintains and governs specifications

Properties of Trusted Electronics

Specification: Challenges

2. The hardware must comply to a **known and complete specification**.

Functionality should not deviate from the specification.

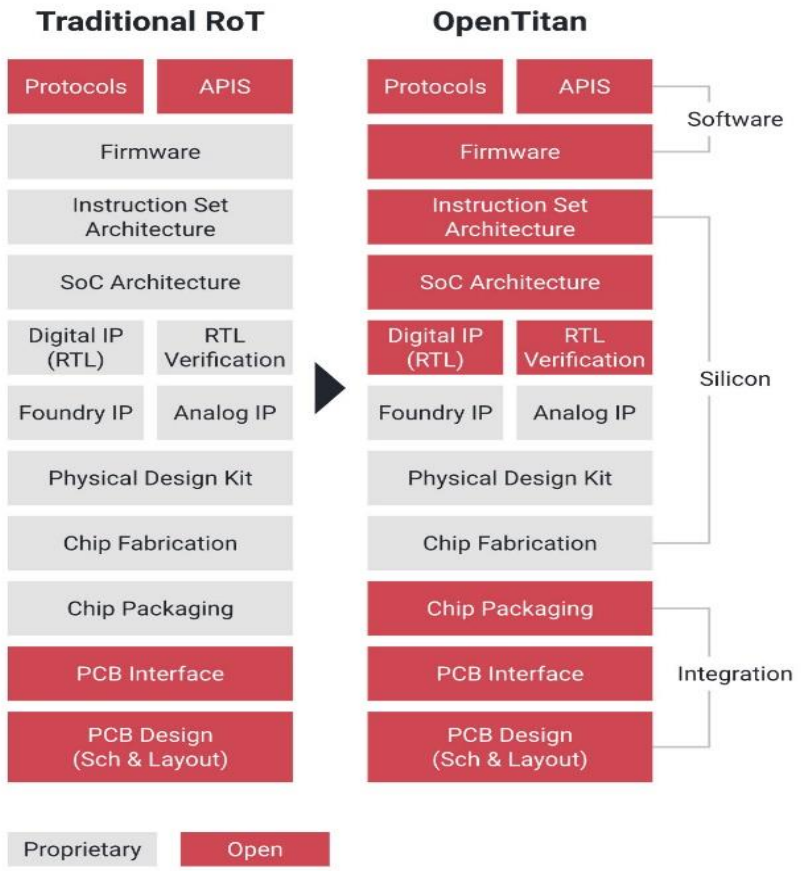
1. Deviations in vendor-specific implementations, customizations or specific extensions
2. Effort for (formal) verification
3. Electronic Value Chain still not entirely open source, Verification of physical chip difficult

Properties of Trusted Electronics

Specification: Challenges

2. The hardware must comply to a **known and complete specification**.

Functionality should not deviate from the specification.



Properties of Trusted Electronics

Hardened against Attacks

3. The hardware must be sufficiently **hardened against attacks.**

Mechanisms to ensure security and avoid vulnerabilities should be in place.

1. **Community Approach:** bug hunting, and many eyes helps security
2. **Driver for Research:** RISC-V spawned research into hardware based security features
3. **Security Features**: Cryptographic Extensions, Memory Protection, etc. provide building blocks of secure systems
4. **Side-channel / Fault Attack Countermeasures**

Properties of Trusted Electronics

Hardened against Attacks: Challenges

3. The hardware must be sufficiently **hardened against attacks.**

Mechanisms to ensure security and avoid vulnerabilities should be in place.

1. Effort for hardening

2. Open-source can expose the architecture to potential exploitation:

   - Vectors for attacks on end-product
   - Vector for attacks in the supply chain (Hardware Trojan Insertion, IP Theft)

Properties of Trusted Electronics

Hardened against Attacks: Challenges

3. Th

Sy

However: long term, security improves with open-source approach

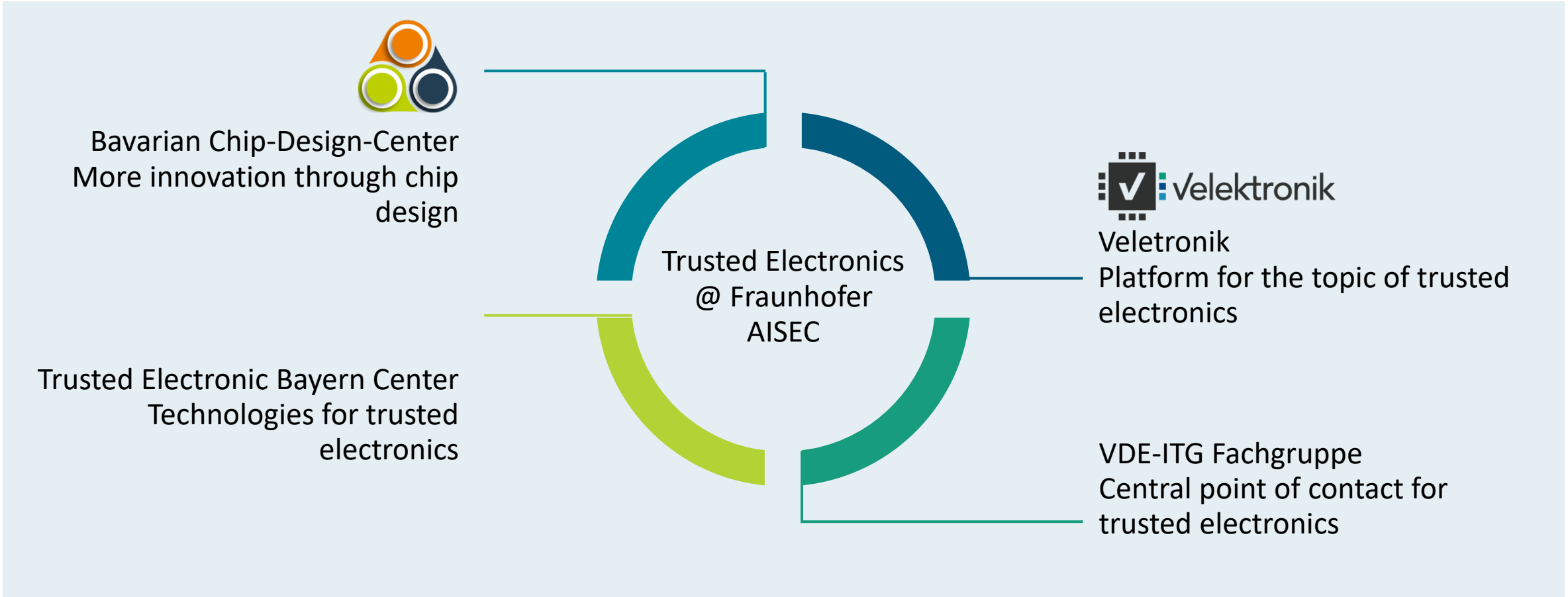
1 Effort for hardening

2 Open-source can expose the architecture to potential exploitation:

- Vectors for attacks on end-product
- Vector for attacks in the supply chain (Hardware Trojan Insertion, IP Theft)

Trusted Electronics @ Fraunhofer AISEC

What are we doing to help



Conclusion and Outlook

Trusted Electronics are a prerequisite for Technological Sovereignty

Hardware Security solutions for RISC-V are an important first step towards trusted electronics…

… however more innovation and research is required.

RISC-V and the Open-Source Ecosystem are a driver for research and innovation in this field, leading to better and sustainable solutions in the long term.

Outlook: new regulation and standardisation, e.g. Cyber Resilience Act

Conclusion and Outlook

Contact

Johanna Baehr

Hardware Security
Tel.: +49 89 3229986-1006
Johanna.Baehr@aisec.fraunhofer.de

Fraunhofer-Institut für Angewandte und Integrierte Sicherheit AISEC
Lichtenbergstraße 11
85748 Garching (bei München)
www.aisec.fraunhofer.de

Fraunhofer
AISEC

Fraunhofer Institute for Applied
and Integrated Security AISEC