Velektronik

Platform for Trustworthy Electronics

Fraunhofer
Forschungsfabrik Mikroelektronik Deutschland
edacentrum
gefördert vom
Bundesministerium für Bildung und Forschung

Project Overview

- ZEUS[1]
  - National funding call dedicated to trustworthy electronics
  - Funded by Federal Ministry of Education and Research (BMBF)[2]
  - 14 projects, 83M€ total budget, 74% average funding rate
- VE-Velektronik
  - 15 partners: Fraunhofer, Leibnitz, edacentrum
  - 6M€, 2021 – 2024
  - https://www.velektronik.de/en/

[1] https://www.elektronikforschung.de/foerderung/bekanntmachungen/zeus (only in German)
[2] https://www.bmbf.de/bmbf/en/home/home_node.html

Project Overview

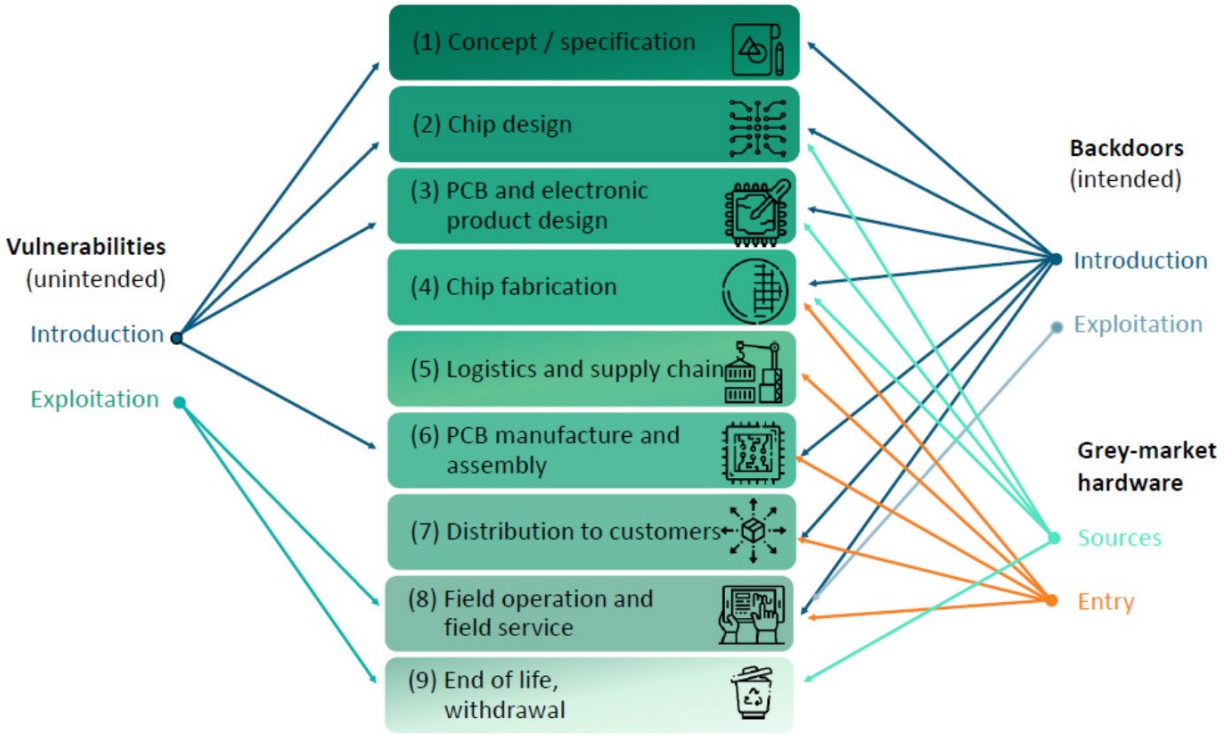
- Goals
  - Identify challenges and solutions within electronics value chain
  - Provide a national platform to connect stakeholders
- Tools
  - Yearly national symposium on trustworthy electronics[1]
    - March 9th - 10th 2022
    - Digital, ~200 participants
  - Reference paper on trustworthy electronics[2]
  - Workshops on chip design, manufacturing, and analysis

[1] https://www.elektronikforschung.de/fokusthemen/vertrauenswuerdigkeit/digitale-fachkonferenz-vertrauenswuerdige-elektronik-2022 (only in German)
[2] https://www.velektronik.de/wp-content/uploads/2022/09/Referenzpapier_Vertrauenswuerdige_Elektronik.pdf (English version available)

Definition: Trustworthy Electronics

1. The hardware must meet **high levels of quality and reliability**.
   - Reliable operation in the field over its full lifetime.
2. The hardware must comply to a **known and complete specification**.
   - Functionality cannot be altered from the specification.
3. The hardware must be sufficiently **hardened against attacks**.
   - Mechanisms to ensure security and avoid vulnerabilities.

Value Chain and Trust Issues



Setting Priorities

- Risk analysis
  - **Severity** – prospective damage
  - **Probability of occurrence** – practical relevance
  - **Benefit / cost ration** – attractiveness for adversaries
- Priorities
  - Three levels: high, medium, low
  - Assessment by experts within Velektronik
  - Reviewed by representatives from research and industry

High-Priority Threats

- **Unintentional vulnerabilities** introduced in **early design steps** and exploited in the field.
- **Intentional backdoors** such as malicious / implant ICs and firmware introduced in **late value chain steps** (e.g. during PCB assembly and logistics).
- **Grey market hardware** through overproduction, use of rejects, and illegal recycling, which infiltrates the value chain at **late value chain steps**.

Assessing Solutions

- **Helpful criteria**
  - Is a high-priority threat addressed?
  - Are significant improvements achieved?
  - What are the necessary expenditures?
- **ZEUS project landscape**
  - All high-priority threats are addressed
  - Least coverage: backdoors in late value chain steps (PCB, assembly, distribution)
  - No coverage: backdoors in early value chain steps (spec, standards, chip design)

Outlook

- **Open questions**
  - Definition precise and comprehensive enough?
  - How to quantify and measure trustworthiness (in each value chain step)?
  - How will trust issues and threats develop?
- **Specific topics**
  - Open(-source) hardware – instruction sets, EDA tools, PDKs, chip components
  - Zero trust – technological vs. organizational measures
- **Next national symposium**
  - Planned for May 2023 in Hannover

Thank you for your attention!

Andreas Seelos-Zankl

Fraunhofer AISEC

andreas.zankl@aisec.fraunhofer.de

https://www.aisec.fraunhofer.de