

Contributions to the APECS Pilot Line: Fraunhofer AISEC

Authors: Dr.-Ing. Matthias Hiller, Dr.-Ing. Nisha Jacob Kabacki

Fraunhofer AISEC is one of 14 German research institutes involved in the implementation of the APECS pilot line. As one of the 12 Fraunhofer institutes, Fraunhofer AISEC's expertise spans integrated security for embedded systems and hardware components, as well as operating systems, applications (apps), and cloud services. Additionally, it offers solutions for secure software and system development and the use of machine learning techniques for cybersecurity.

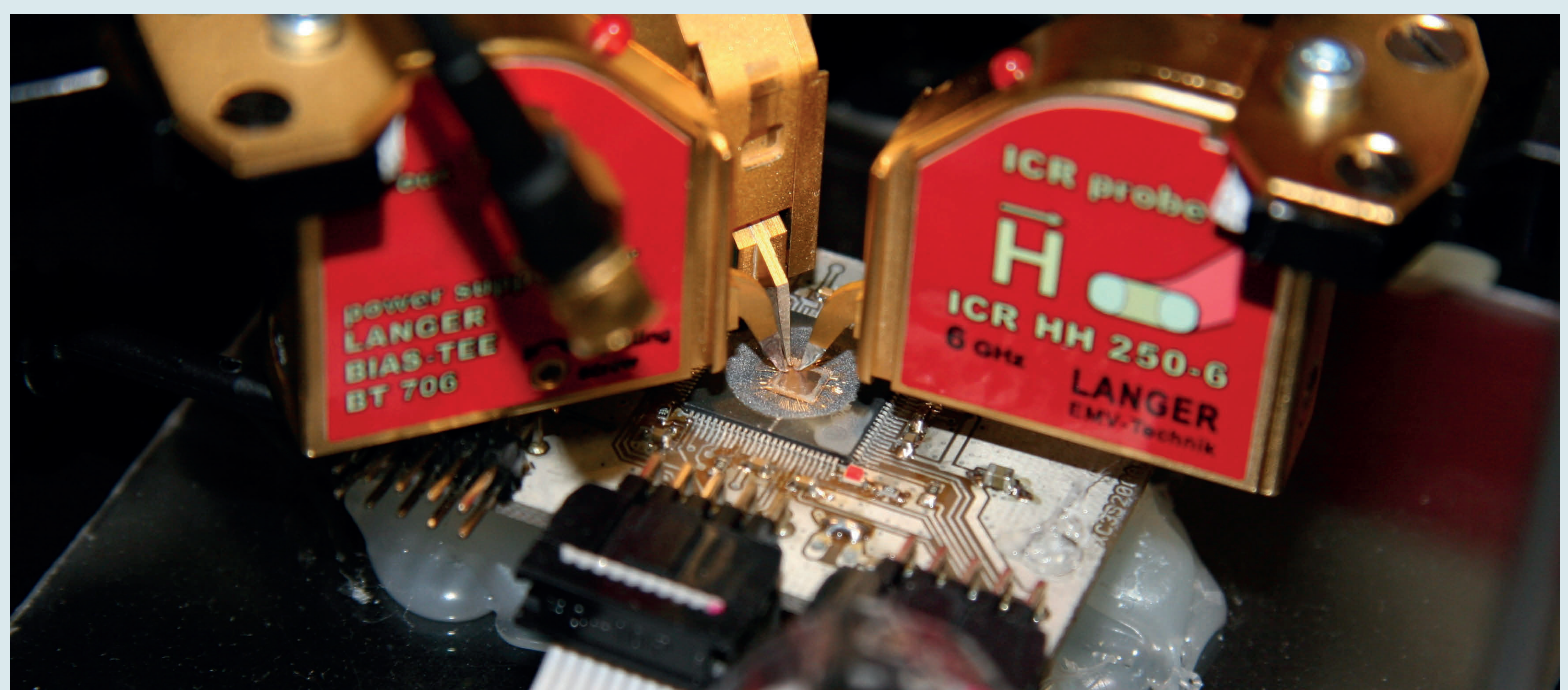
The role of Fraunhofer AISEC in the APECS pilot line

One of the main topics of APECS is Characterization, Test & Reliability (CTR). A major objective of the pilot line is to develop new testing and failure analysis, with trusted electronics at the heart of its work, particularly regarding the security and authenticity of chiplets. Within APECS, Fraunhofer AISEC is contributing to the pilot line, with a strong focus on trusted electronics.

- Development of **security features for chiplets** and execution of security analyses on chiplet-based and heterogeneously integrated systems
- Creation of **innovative hardware trust anchors** for authenticating the chiplet system and its components internally and to third parties. They are a necessary foundation for building a secure and trustworthy overall system
- Analyzing chiplet technologies for **new physical primitives** and designing **proofs of concept** for IP blocks that utilize both established and novel hardware primitives, translating them into chiplet-specific functions
- Research, design, and implementation of **integrated hardware-software security solutions** tailored to RISC-V-based chiplet architectures
- Research, design, and implementation of **security analysis** techniques in a **secure environment**, including preparation and localization of critical components and analysis of actual security functionality

Parallel measurement of the electromagnetic radiation of an integrated circuit with multiple high-precision probes

© Fraunhofer AISEC



RISC-V Secure Element — 'Made in Germany' Security Chip Serves as a Root of Trust for Connected Devices

With the RISC-V Secure Element, Fraunhofer AISEC, IIS, and EMFT created a security chip that was designed and manufactured in **Germany**. The design is based on transparent **open-source hardware** and integrates **post-quantum cryptography**. It can be used as a **standalone chip** or as a **system-on-chip component** and serves as foundation for the **security chiplet** designed in APECS.

The goal is to offer companies a trustworthy and customizable **trust anchor — with points of contact in the EU** — for connected devices and to support them in addressing increasing cybersecurity threats and the resulting requirements to mitigate them.

Variants with specialized accelerators, interfaces or additional security features can be produced even in **small and medium quantities** or integrated as a customer-specific root of trust into a larger chiplet system.

Optical Analysis for Chiplet Security Evaluation

The rapid adoption of chiplet-based heterogeneous integration is replacing system-on-chips (SoCs) with decomposed multi-die assemblies. This introduces a largely uncharted hardware security surface, as interposers, bridges, redistribution layers, and die-to-die interconnects may expose sensitive internal structures and traffic.

Fraunhofer AISEC is currently systematically **mapping chiplet-specific security threats** to the most common established **optical analysis methods**, e.g., Laser Voltage Probing (LVP), Photon Emission Microscopy (PEM), Electro-optical frequency mapping (EOFM), and Lock-in Thermography (LIT) to threat vectors, clarifying which method is applicable for which security evaluation purpose.

What is APECS?

APECS (Advanced Packaging and Heterogeneous Integration for Electronic Components and Systems) is one of 5 European pilot lines established under the EU Chips Act. APECS is the foundation for Europe's competitive position in heterogeneous system integration and advanced packaging. It plays a vital role in enhancing Europe's strategic autonomy by reducing dependence on foreign suppliers and strengthening Europe's capabilities in critical technology areas.

Contact

Dr.-Ing. Matthias Hiller
Phone +49 89 3229986-162
Email: matthias.hiller@aisec.Fraunhofer.de

Dr.-Ing. Nisha Jacob Kabacki
Phone +49 89 3229986-116
Email: nisha.jacob@aisec.Fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security
Lichtenbergstraße 11
85748 Garching near Munich, Germany
www.apecs.eu | info@apecs.eu

Additional information

The work presented was carried out in the framework of the APECS Pilot Line of the Chips Joint Undertaking, funded by Horizon Europe and Digital Europe Programmes and national funding authorities of Austria, Belgium, Finland, France, Germany, Greece, Portugal, Spain.

Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the Chips Joint Undertaking. Neither the European Union nor the granting authority can be held responsible for them.

RISC-V Secure Element

