

# Trustworthy microelectronics: key technology for digital value creation

Microelectronics is a key technology for digitalisation. Fraunhofer AISEC is conducting research into trustworthy microelectronics in collaboration with partners, thereby promoting competitiveness and technological sovereignty.

Smartphones, industrial manufacturing, and medical diagnostics would be unthinkable without microchips. This makes it all the more important that electronics are reliable and trustworthy. In light of growing cyber threats, which are being addressed by EU regulations such as the Cyber Resilience Act (CRA), companies need to secure their products and supply chains at the hardware level as well.

## Initiative for Trusted Electronics

In cooperation with the Association for Electrical, Electronic and Information Technologies (VDE) and the research platform 'Velektronik', the VDE specialist group 'Trustworthy Electronics' was established in 2024. It serves as a central point of contact for promoting trustworthy electronics in a network of industry, research, and public authorities in Germany. The aim is to jointly raise awareness of trustworthy electronics, help shape industry standards and develop new security approaches. Prof. Dr. Georg Sigl, Director of Fraunhofer AISEC, is the spokesperson for the initiative.

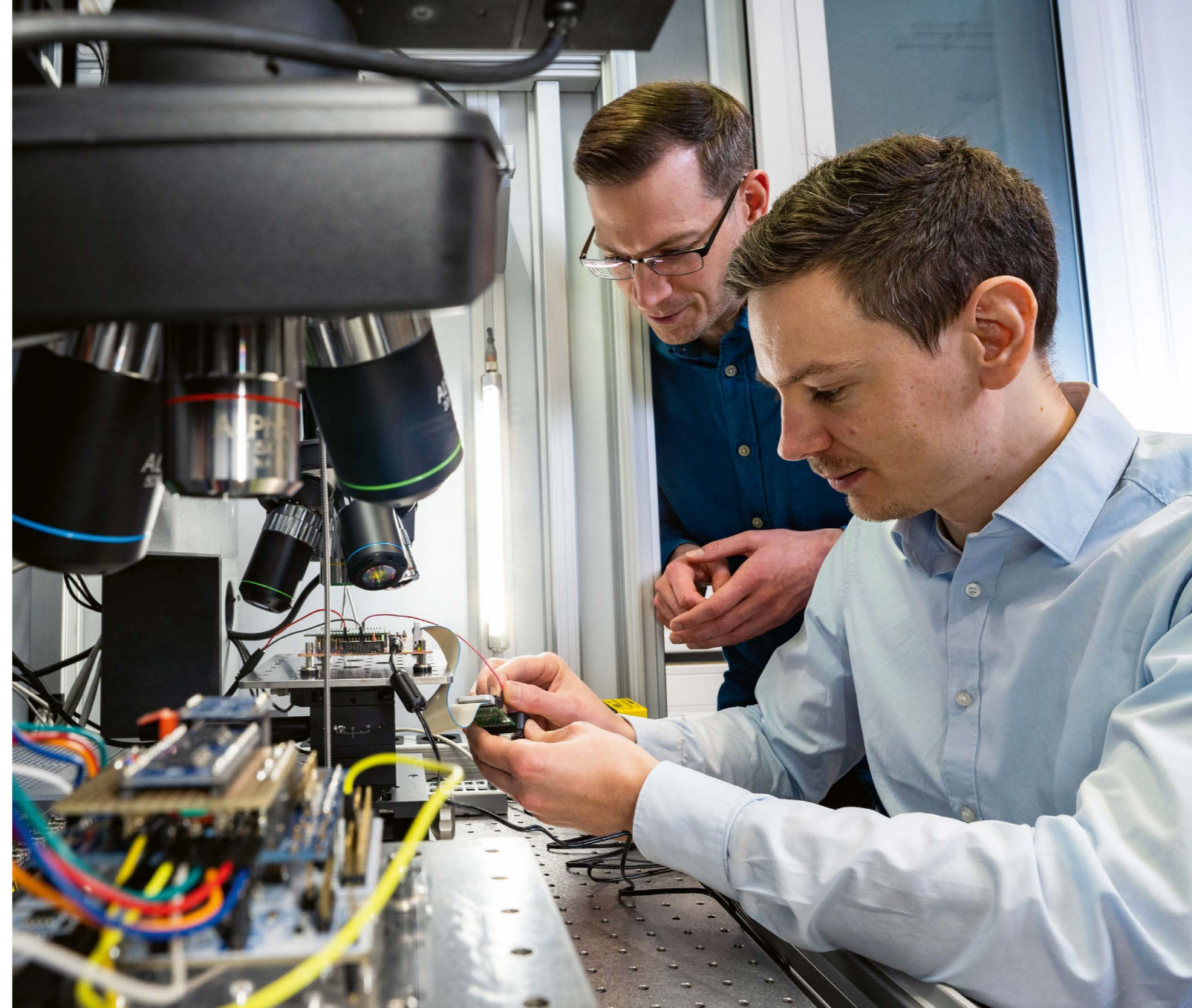
The focus is on sharing new research findings and best practices between universities, industry, testing laboratories and public authorities. The expert group monitors legal requirements such as NIS-2 and CRA, analyses new security incidents in the field of trusted electronics and initiates projects that contribute to the further development of secure electronics.

## Bavarian Chip Design Centre as a driver of innovation

Another key project aimed at strengthening the semiconductor industry is the Bavarian Chip Design Centre (BCDC), funded by the Bavarian State Ministry of Economic Affairs, Regional Development and Energy. The BCDC aims to strengthen Bavaria as a location for innovation in chip design and facilitate access to strategically important technology for small and medium-sized enterprises (SMEs) and start-ups.

Researchers at Fraunhofer AISEC are developing new security architectures for trustworthy electronics and hardened processors based on open RISC-V designs. The close integration of hardware and software creates protected environments based on mechanisms such as trusted execution environments and confidential computing. In addition, verified boot processes, secure firmware updates and architecture-based security measures ensure robust protection against attacks on software vulnerabilities.

Through its active contribution to the VDE expert group and the BCDC, Fraunhofer AISEC strengthens the competitiveness and technological sovereignty of the Bavarian, German and European semiconductor industry and establishes trustworthy electronics as a key technology for a secure digital transformation.



## Contact

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

## Fraunhofer AISEC as a network partner for promoting trustworthy hardware



Press release 'VDE expert group'



Press release 'Bavarian Chip-Design-Center (BCDC)'



Department 'Hardware Security'