The Internet of Things is increasingly pervading industrial and personal applications, including, for example, smart meters and smart grids, industrial and process automation, Car-to-Car and Car-to-X communication, home and building automation, telehealth and telecare applications. Wired and wireless networks of embedded systems, as well as their interconnection in “cyber-physical systems” (CPS) are playing an increasingly important role in this context. As more and more systems perform functionally critical tasks autonomously, their reliability and security are also continuing to gain in importance. Consequently, data security and privacy aspects need to be addressed.

The Institute of Reliable Embedded Systems and Communication Electronics (ivESK) at Hochschule Offenburg was formed to focus on these issues. We are especially active in the following areas:

- Conception and implementation of efficient and modular, wired and wireless communications protocols using embedded systems
  - e.g. with 6LoWPAN, Wireless M-Bus, M-Bus
- Conception and implementation of integrated security architectures for communications solutions using embedded systems
  - e.g. embedded TLS1.2, PKI solutions for distributed applications
- Conception and implementation of efficient and secure, embedded computing platforms
  - e.g. Embedded Linux (SpeedBoot, virtualization)
- Testing and verification of communications solutions
  - e.g. with automated physical testbed (APTB)
  - e.g. with network simulation and emulation
- End-to-end security solutions between resource-restricted devices and powerful components, and connection to a cloud ecosystem