About the Project

Many modern applications such as highly automated driving or flexible production facilities are based on complex electronic systems. These electronic components are making our lives and work ever easier, safer, more environmentally friendly and more pleasant. However, they also pose a potential danger if these systems are not developed with the clear goal of trustworthiness from the outset.

Against this background, the Federal Ministry of Education and Research (BMBF) has launched the funding measure "Trustworthy Electronics (ZEUS)", within the framework of which the research project "Design Methods and HW/SW Co-Verification for the Unambiguous Identifiability of Electronic Components" (HoLoDEC) has been working since March 2021. HoLoDEC aims to systematically identify all potential security vulnerabilities already in the design stage and to protect electronic systems from attacks using automatically generated, reliable mechanisms. HoLoDEC focuses on assuring the trustworthiness of the system hardware (HW) and takes into account the direct interfaces to trustworthy software/firmware components.

Already during design at the architectural level, the trustworthiness of a system must be planned and ensured for all subcomponents. Therefore, HoLoDEC researches trustworthy development and verification processes that arm electronic systems against attacks in a verifiable and, if possible, quantifiable manner. The design methods, tool chains and test suites that are being created in this joint project are intended to form a solid basis for future development tools for trustworthy electronics and thus contribute to the technical and technological sovereignty of Germany and Europe.

Major attack scenarios on electronic systems are:

- attacks via the Internet ("hacking"), in which intentionally introduced backdoors and Trojans or accidentally left vulnerabilities are used to change the functionality of the system or steal data stored in it;
- Electronic, optical and physical attacks on integrated circuits to steal intellectual property or illegally read or modify data.

The leading cyber vulnerability cataloguing institution (CVE-MITRE) estimates that overall system vulnerability can be reduced by 43 % if trustworthiness vulnerabilities are removed at the hardware level. Approaches at the system level currently help to ward off attacks and reduce security risks, these include access restriction or redundancy. HoLoDEC starts here with a holistic security concept to improve the development processes for trustworthy electronic systems and their integration along the global value chains. The basis for this is a novel IP design and verification flow that will ensure trustworthiness, especially in safety-critical electronic systems.

HoLoDEC works in an application-oriented manner and brings together companies from important sectors such as automotive and Industry 4.0 with supplier companies, development and research partners.

Das Projekt HoLoDEC wird unter den Förderkennzeichen 16ME0695K-16ME0705 im Förderprogramm IKT 2020 durch das Bundesministerium für Bildung und Forschung (BMBF) gefördert.
