*H*ardening the Value Chain through Open Source, Trustworthy *E*DA tools and *P*rocessors

The HEP research project in a nutshell

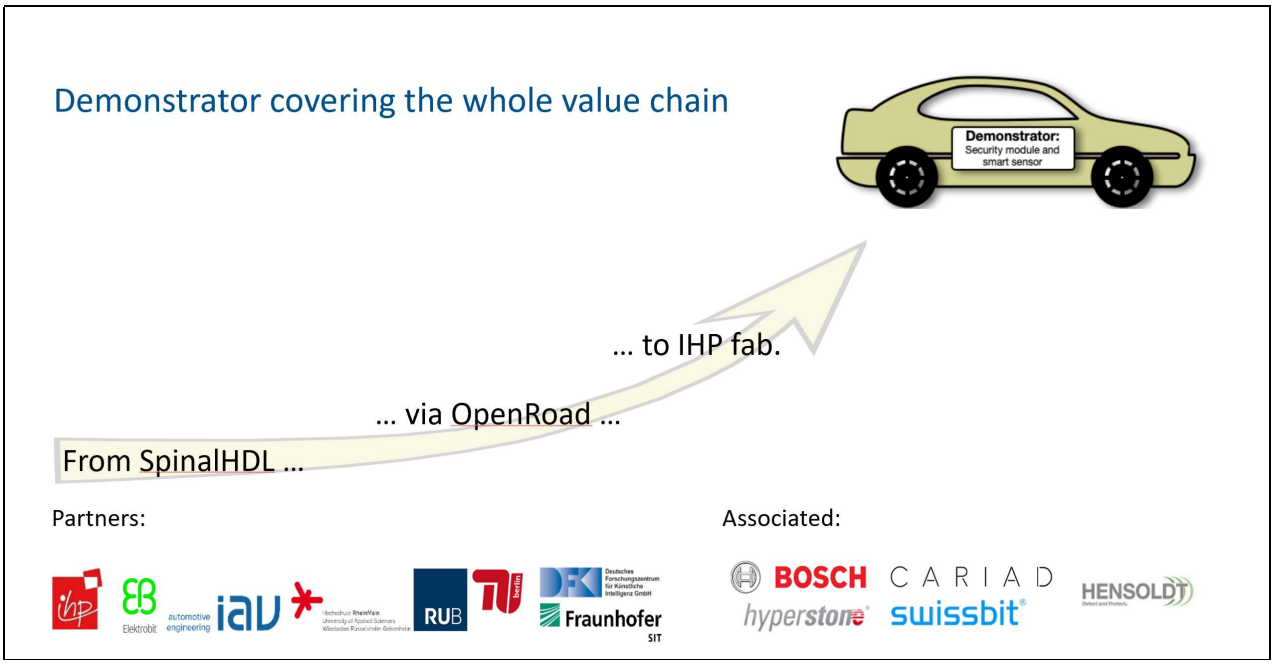
Project HEP conducts research on designing an open hardware security module, using an open design flow, and performing mathematical proofs of correctness.

We address the following problems:

1. Security: An open system is created, with flexible means against side-channel attacks and a formally verified processor.
2. Sovereignty: Users are given control over the components used.
3. Costs: These are reduced due to lower license costs for components and tools.
4. Lack of innovation: The ASIC development process is opened to a broader community.

Open-source hardware and design tools are already being used in production today, e.g.

- the Titan chip was developed by Google using the open *Risc-V* processor design;
- the use of the open-source synthesis tool *Yosys* by Renesas Electronics; and
- the open-source behavioral model tool *Verilator* by NXP.



Our project builds on tools similar to those used in the OpenLane project, partially funded by US DARPA. Thus, we aim to establish an open ASIC design flow freely available in Europe, including a partner semiconductor fabrication facility, IHP. We are similar to the Google Sky130 project with the efabless company and the Skywater fab.

To increase security, we are co-operating with the creators of SpinalHDL. As a first result, SpinalHDL now offers advanced features for cryptographic designs that allow the semi-automated integration of countermeasures against side-channel attacks. Furthermore, project HEP will use the award-winning VexRiscv processor design. Its implementation will be formally verified. In fact, the entire semiconductor production chain should be open. Unfortunately, there is no European fab currently providing an open-source process design kit to unlock the potential of an open-source ASIC design flow fully. We are working on this issue.

We are a consortium of six research partners, two industrial partners from the automotive industry, and five associated partners working in hardware and chip design security solutions.

Our next steps will be to provide an FPGA prototype code in 2022 and an ASIC-design in 2023. We will thereby demonstrate that open components and tools foster trustworthiness and innovation.

More information

http://hep-alliance.org/

Contact

Norbert Herfurth, Leibniz Institute for High Performance Microelectronics (IHP), Frankfurt (Oder), Germany, email: herfurth@ihp-microelectronics.com

Arnd Weber, contractor of the Technical University of Berlin, Department Security in Telecommunications, Germany, email: arndwweber@gmail.com

Supported by

Bundesministerium
für Bildung
und Forschung