

Secure remote activation for machine tools – quantum-safe and future-proof

How can machine tools be activated remotely and securely? The 'PoQsiKom' project has developed a crypto-agile, quantum-safe technology that can withstand future threats. A specially secured chip enables the reliable verification and activation of safety devices across national borders.

In industry, machine tools are typically used for decades, which is why their safety must be guaranteed in the long term. Since quantum computers may be able to break classic encryption methods in the future, it is essential to switch to quantum-safe communication between different components in industrial engineering today in order to permanently protect sensitive production data and control processes.

The growing trend towards intelligent manufacturing is leading to increased communication between different components in industrial engineering. As communication increasingly takes place beyond the boundaries of one's own trust domain, e.g. in international cooperation, authenticated and secure communication connections are no longer sufficient. It is also necessary to verify the trustworthiness of the data generated and exchanged on the devices.

Security primitive grants trustworthiness of critical data

The 'PoQsiKom' project (post-quantum secure communication for Industry 4.0) has developed a concept that enables the secure remote activation of protective areas on machine tools. This is based on a chip with crypto-agile, quantum-safe security technology that can be used flexibly and will also withstand future threats.

Until now, safety devices on machine tools have been activated locally by physically present persons via directly wired terminals. The safety area of the machine tool is protected by light barriers. If the light barriers are interrupted, e.g. by third parties, animals or objects, the machine is stopped. The machine may only be restarted after activation by a trained person. Until now, this had to be done by personal inspection on site. In contrast to personal inspection, remote access places higher demands on the availability, authenticity, integrity and confidentiality of the data used.

By implementing cryptographic building blocks, also known as security primitives, in each individual device, it is now possible to activate security features remotely across national borders. The crypto-agile and quantum-safe security chip forms the trust anchor and is already integrated into the device design. A real-time-capable operating system hardened against malware prevents data from being compromised during processing. In addition, the security technology guarantees that remote systems remain in the correct and unaltered state.



Research and industry working hand in hand

In the 'PoQsiKom' project, TU Munich is responsible for the FPGA-based hardware platform for the trust anchor and, together with Siemens AG, for implementing the cryptographic post-quantum algorithms. Fraunhofer AISEC is responsible for securing the real-time operating system, while Siemens AG is leading the development and standardisation of the GTA API. The high-tech company TRUMPF is developing a concept for the release of safety devices via the Internet and is implementing this in a demonstrator using the trust anchor developed in the project for secure communication.



Contact

Bartol Filipovic

Head of Department Product Protection and Industrial Security
Phone: +49 89 3229986-128
bartol.filipovic@aisec.fraunhofer.de

More Information



Project 'PoQsiKom'



Department 'Product Protection and Industrial Security'