Fraunhofer SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY

Fraunhofer Institute for Secure Information Technology SIT

Contact:
Dr. Kpatcha Bayarou
Rheinstraße 75
64295 Darmstadt
Germany

Phone +49 6151 869-274
Fax +49 6151 869-224
kpatcha.bayarou@sit.fraunhofer.de
www.sit.fraunhofer.de

ANTI-PIRACY PROTECTION

FOR MOTION CONTROL APPLICATIONS

The German mechanical engineering industry is a worldwide leader. Fraunhofer SIT supports machinery engineers and component manufacturers in the active protection of their expertise and offers ready-to-use solutions for the combat against product counterfeiting and industrial espionage.

In emerging economies machinery engineers make high profits, but the risk of product counterfeit is just as high in these countries. The illegal reproduction of plants, systems or components is increasingly threatening to the mechanical engineering industry and results in enormous economic damage. According to VDMA German companies alone sustain a damage of approx. 7.9 billion Euros per year. Machines are not only being copied, sometimes they are distributed as the faked originals of recognized brand name companies. Product counterfeiters even offer repair and maintenance services with counterfeited modules. These kind of services are required for larger machineries that perform coordinated multiple motion sequences. Since the sheer wear on the components makes it necessary for the facility operator to exchange them from time to time and to service the plant on a regular basis, it is particularly important in the motion control application field that even individual, retrofitted components can be marked distinctly as the original products.

Current concepts are often based on obfuscation mechanisms (e. g. code obfuscation) or inflexible physical guarding measures (e. g. hardware dongle). Code obfuscation aims at making the program flow logic appear incomprehensible. It increases the effort for retrofitting, but does not offer an effective protection against illegal copies. Combining code obfuscation and a hardware module (dongle) protects only the software of the control unit, but does not prevent hardware copies. The protection concepts developed at Fraunhofer SIT are entirely different. They protect both machine data and software against unauthorized transfers, and components against successful replication (based on reverse engineering attacks on individual components or the entire system) as well.

Protection for Plant Engineers and Component Manufacturers

The security of the solution concepts offered by Fraunhofer SIT rests on the system component identification by means of secret codes and state-of-the-art crypto procedure implementation. Specifically, it is a combination of software and hardware elements. Without access to the machine’s secret codes, even company insiders, who know the system very well and may have been involved in its construction, cannot counterfeit individual modules or the central control unit. The main concept developed at Fraunhofer SIT is based on guidelines from the Federal Office for Information Security. Its integration into existing machinery is very cost-efficient, because production processes, operating procedures and maintenance sequences do not need to be modified. The protection level can be adjusted in such a manner that no disruptions may occur due to unintentional or short-term changes on individual components.

Recognizing Fakes

The component recognition is founded on the linking of individual cryptographic identities to existing system components. For proper machine operation the desired components must be licensed beforehand, and later pass authorization at a central control unit. Component manufacturers and plant engineers may realize the piracy protection jointly or separately. The Fraunhofer SIT system protects individual components as well as assembled systems. The security concepts are customized according to the individual user's request and take the relevant parameters from the respective application case (e. g. amount and security criticality of the accrued data) into consideration.

Forged system components will be detected immediately. Accordingly, machines will function faultlessly only if the components used are authentic and have been licensed by the manufacturer. If individual system components malfunction they can be replaced by new, properly licensed components at any time, without having to reinitialize the entire system. At the same time the system is open and flexible. Sublicenses (in the form of a certified code) may be issued to other component manufacturers, which allows these manufacturers to integrate their own products without impairing the overall system's anti-piracy protection. Hardware and software modules can be adapted to the requirements of the application context by implementing only the functionalities specifically desired or required. Unnecessarily complicated or cost-intensive (for the actual application case possibly not indicated) security modules can be avoided. This facilitates the exploitation of export opportunities and the efficient protection of manufacturer and machine engineering knowledge.

Our service offer

Fraunhofer SIT supports facility operators and component manufacturers in the safeguarding of components and systems.

We offer:

- Consultation services about technological anti-piracy protection
- Development of individual security concepts
- Development of threat models and test scenarios
- Piloting and feasibility studies
- Evaluation and further development of existing protection concepts