

INDUSTRIAL SECURITY



TRENDS

Companies in the manufacturing industry have always wanted to optimize their machine load, minimize their inventory, and improve their energy efficiency in order to maximize productivity and maintain their competitiveness. As a result of growing interconnectedness, production systems are becoming a part of industrial environments with connections to ERP systems and other IT office applications.

Machine Communication

Components and equipment are increasingly outfitted with IuK technology. Cyber Physical Systems, i.e. systems of systems, develop out of previously isolated units. Via IT technology, these systems are capable of communicating with each other and processing information about production processes, the products themselves, as well as logistics chains.

Big Data

Through the increased use of sensors, the amount of information in production environments is growing. As a result, production is not only able to be monitored meticulously, product history can be followed reliably and establish secure legal evidence – even off-site.

CHALLENGES

The growing complexity of industrial processes only presents one of the new dangers accompanying changes in the industrial sector. Massive IT interconnectedness via the internet is making production technology systems and the products manufactured within them attractive targets for industrial espionage, sabotage, and organized cyber criminals. Machine-specific attacks via Trojans, for example Stuxnet, Duqu, Flame, Shamoon, or the most recent activities of diverse intelligence services, like Prism, Byzantine, ShadyRat or Tempora, have already shown that extremely real threats exist.

Protection of Know-how and Manufacturing Knowledge

Considering the possible information channels within production environments, there is a growing necessity to protect valuable know-how and unique product characteristics without inhibiting manufacturing processes and quality. The goods that are to be protected as well as the processes and data differ incredibly. For instance, machine and systems manufacturers are concerned about piracy prevention as well as protecting machine configurations and settings.



SERVICES

Fraunhofer SIT has longstanding experience in the conception and realization of cryptographic concepts that enable software and hardware elements to be connected with each other as required for each individual application. The Institute runs its own test laboratory, where comprehensive security evaluations are performed based on national and international standards as well as in accordance with the Institute's own seal of approval.

Fraunhofer SIT offers the following services to companies in the production field:

- Creation of threat analyses and minimum requirements
- IT security evaluation of systems and components
- Integration of IT security mechanisms
- Development of protocols and IT security functions
- Development of security architectures for industrial networks
- Product protection via cryptographic systems
- Secure engineering for software development processes
- Technical consultation

BENEFITS

For system operators:

- Protection against production losses and problems
- Fast and efficient support with risk management

For system/machine/component manufacturers:

- Competitive advantages via certified security properties
- Protection against product piracy and reverse engineering

REFERENCES

Protection against Piracy for Equipment

On behalf of an industry partner, Fraunhofer SIT has developed a concept protecting equipment from unauthorized manipulation and reverse engineering. The system was implemented with the help of proven cryptographic processes. Even insiders are unable to tamper with components and control units without access to the secret code.

Trusted Core Network

In cooperation with industry partners, Fraunhofer SIT has developed the Trusted Core Network (TCN). This network is capable of checking the identity of network nodes and guaranteeing they are in a predetermined condition.

Pharmaceutical Identification & Compatibility Tool (PIC)

PIC is a low cost RFID tag based solution to verify the authenticity of products in pharmaceutical supply chains. With this tool, all participants in the supply chain are able to verify a product's authenticity and specify its next recipient simply by using an NFC capable mobile phone.

ContainIT – Secure IT Infrastructure for Logistics

The development of an IT infrastructure that integrates the multitude of partial applications and processes of container logistics and increases efficiency and security. Fraunhofer SIT evaluated the telemetric systems and sensor technology for monitoring the container status.

THE INSTITUTE

Information technology has already permeated large parts of our everyday life: whether it be a car, telephone or heating. Without the use of IT, the majority of devices and systems are almost inconceivable. Businesses in particular use IT systems to effectively design their working processes. The Fraunhofer Institute for Secure Information Technology focuses on protecting these systems against failures, attacks and manipulations.

The Institute works for companies in various industries. Many successful projects with international partners are impressive evidence of the faithful and reliable cooperation. Our customers include HP, Software AG, SAP, Lufthansa and the Federal Office for Information Security.

CONTACT

Dr. Thorsten Henkel

Phone +49 6151 869-4271

Fax +49 6151 869-224

thorsten.henkel@sit.fraunhofer.de

Fraunhofer Institute for Secure Information Technology

Rheinstrasse 75

64295 Darmstadt, Germany

www.sit.fraunhofer.de