

RESEARCH NEWS

April 2017 || Page 1 | 3

Hannover Messe 2017 – Industrie 4.0 production facilities

New security procedures secure the intelligent factory

At the Hannover Messe from April 24 to 28, 2017, Fraunhofer researchers will present two new procedures for the protection of Industrie 4.0 production facilities (Hall 2, Booth C16/C22): here, a self-learning system recognizes security incidents in manufacturing facilities without knowledge of the underlying system architecture. Hardware-based security modules report manipulation tests on machines and components.

Manufacturing processes in the context of Industrie 4.0 are highly automated: the realization of the customer's request is triggered as an assignment by the merchandise management system, the components required for the product are provided by the supply chain and the construction plans as well as the exact production procedure are retrieved from the supplier. Manufacturing occurs worldwide in order to be able to deliver as quickly as possible and without long distances.

However, these very flexible, individual and IT-dependent production processes increase the risk of manipulation in the production process, inferior or falsified components, or loss of know-how through product piracy. To protect against this, all data and communication channels used in the production process have to be secured and IT security has to be enhanced.

Identifying irregularities, ensuring quality

At the Hannover Messe 2017, the Fraunhofer Institute for Secure Information Technology SIT in Darmstadt demonstrates two procedures that use new approaches in the protection of industrial facilities. The first is to detect irregularities in the communication networks of manufacturing facilities, and the second is to ensure the integrity of the components involved in the manufacturing process and, as a result, the quality of the data and products they produce.

To detect anomalies during the operation of a plant, a self-learning system is used which analyzes data flows from all entities involved in the manufacturing process, such as sensor, design and order data, as well as personal data (if applicable). After a learning phase, it detects whether certain processes in the network belong to normal operation or represent a deviation from it – initially regardless of whether or not an attack is involved. The monitoring system oversees the architecture of the network and the allowed access paths via software defined networking (SDN). By analyzing com-

Contact

Janis Eitner | Fraunhofer-Gesellschaft, München | Communications | Phone +49 89 1205-1333 | presse@zv.fraunhofer.de

Oliver Küch | Fraunhofer Institute for Secure Information Technology SIT | Phone +49 6151 869-213 |
Rheinstrasse 75 | 64295 Darmstadt | www.sit.fraunhofer.de | oliver.kuech@sit.fraunhofer.de

munication and data, the system is able to recognize, for example, whether certain components behave unusually or whether larger amounts of data flow in a particular direction.

A second method monitors the software condition of components and machines. If these are manipulated in an unauthorized manner, integrity monitoring will sound an alarm. It combines software and hardware elements in order to determine the current state of a component even from far away. By assuring that components are in an expected and safe condition, the system also ensures the quality of the data that is used in the process. In case of detected attacks, plant operators can return infected components via the network to a trustworthy state without a technician having to interact directly with the component. This reduces costs and improves risk management considerably.

Industrie 4.0 needs new security procedures

"The methods known from classical IT, such as virus scanners or intrusion detection systems, are usually not suitable for production facilities," says Dr.-Ing. Thorsten Henkel, who is responsible for Industrial Security Solutions at the Fraunhofer Institute for Secure Information Technology (SIT) in Darmstadt. On the one hand, they are not fast enough to meet the requirements of industrial facilities in terms of availability; on the other, they assume that the environment they monitor and their normal operating conditions are as well known as the methods of their potential attackers.

But exactly this is not the case with the production facilities of the future. "Production in the context of Industrie 4.0 is agile and constantly changes its architecture; it is decentrally organized and largely autonomous," says Henkel. For this reason, security mechanisms and network concepts are necessary which work independently of architecture and allow for the degrees of freedom intended by Industrie 4.0 facilities.

Project IUNO

The Fraunhofer SIT's procedures for the safeguarding of Industrie 4.0 production facilities are partly developed within the framework of the IUNO project (initiated by the Federal Ministry of Education and Research) which is devoted to IT security in Industrie 4.0 and is due to be finalized in mid-2018.

RESEARCH NEWS

April 2017 || Page 3 | 3



At the Hannover Messe 2017, the Fraunhofer SIT demonstrates two procedures that use new approaches in the protection of industrial facilities. The first detects irregularities in the communication networks. The second ensures the integrity of the components involved in the manufacturing process. (© Fraunhofer SIT/CC BY-SA 3.0) | Picture in color and printing quality: www.fraunhofer.de/en/press

The **Fraunhofer-Gesellschaft** is the leading organization for applied research in Europe. Its research activities are conducted by 69 institutes and research units at locations throughout Germany. The Fraunhofer-Gesellschaft employs a staff of 24,500, who work with an annual research budget totaling 2.1 billion euros. Of this sum, 1.9 billion euros is generated through contract research. More than 70 percent of the Fraunhofer-Gesellschaft's contract research revenue is derived from contracts with industry and from publicly financed research projects. International collaborations with excellent research partners and innovative companies around the world ensure direct access to regions of the greatest importance to present and future scientific progress and economic development.