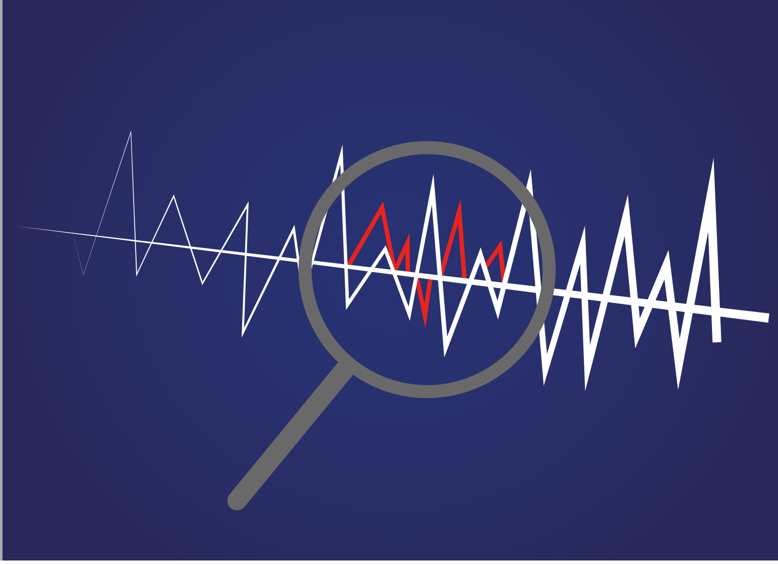
Fraunhofer
SIT

FRAUNHOFER INSTITUTE FOR
SECURE INFORMATION TECHNOLOGY



# EARLY WARNINGS FOR INDUSTRIAL NETWORKS

## DETECT THREATS, FEND OFF ATTACKS, SAFEGUARD NETWORKS

*Fraunhofer Institute for Secure
Information Technology SIT*

*Contact:
Sinisa Dukanovic
Rheinstrasse 75
64295 Darmstadt
Germany*

*Phone +49 6151 869-153
Fax +49 6151 869-224
sinisa.dukanovic@sit.fraunhofer.de
www.sit.fraunhofer.de*

In an industrial Internet of Things environment many different and interconnected machines communicate with each other. The resulting data flows allow for early threat and anomaly detection: The Fraunhofer SIT experts are using the network traffic of Industrial Control Systems (ICS) as an early warning system for attacks and other undesired modifications by analysing the traffic with methods gleaned from machine learning and big data technologies, thus averting threats to Industrie 4.0 as well as blackouts early on.

Industrial networks consist of many interconnected machines and devices such as routers, plant components, network nodes, switches and other devices, all of which are permanently exchanging data. Most companies have safeguarded their network from the outside by implementing various network security applications, such as firewalls, that are able to detect known threats and protect from common attacks. The detection rate of these applications, however, is rather poor with regard to attacks carried out with new pattern types. Due to increasing numbers of communication participants and increasing network activity resulting in an increased complexity of industrial networks, this complexity is making it difficult to monitor ICS and detect anomalies. This in turn could lead to compromised controls or data theft caused by yet unknown malware without anybody noticing, as it was the case with the computer worms Stuxnet or Duqu, for example.

### Network analysis with artificial intelligence

This is why the Fraunhofer SIT experts are applying methods from machine learning and big data technology in order to identify unknown threats, unauthorized access, network errors and other anomalies within an ICS: Based on the company's normal network, and using machine learning, a model is trained first, which then is used as the starting point for the analytic process. The anomaly detection system takes this model and applies it to the new running network traffic. All data traffic will be included, for example fieldbus data, sensor data, manufacturing or ERP data. If occurrences are detected that deviate from the previously trained model (i.e. represent an anomaly), these occurrences will be identified and reported via a security command centre.

Thus the Fraunhofer SIT is helping network providers to achieve better data flow transparency within their Industrial Control Systems and to detect not only known threats but also previously unknown anomalies that may represent a danger.

### Our offer

- Anomaly detection in ICS using machine learning and big data technology
- Individual network data analysis
- Analysis of fieldbus, sensor, manufacturing and ERP data