PRESS RELEASE

SPS 2024: AI-based Alarm System for OT Networks

Operational Technology (OT) networks are exposed to numerous threats. SSV has implemented an AI-based adaptive sensor system that uses real-time monitoring to automatically detect cyberattacks at a very early stage and alert those responsible.

Hanover, September 2024. Networked assemblies in an Operational Technology (OT) network segment are predominantly weakly protected from a cyber security perspective compared to IT systems. At best, there is a perimeter protection function between the individual network segments, such as a firewall. The OT modules themselves are relatively unprotected against cyber attacks.

SSV wants to change this security-critical situation with a newly developed embedded intrusion detection system (IDS). To do this, a special application - the IDS Data Exploration Tool (IDET) - uses functions from the field of artificial intelligence and machine learning (ML) to learn the normal state of the communication relationships in a network segment or directly at a device interface. The IDET then generates a platform-independent AI model that enables an inference engine to detect anomalies in the network data in real time.

Henrike Gerbothe, the SSV manager responsible for this solution, explains: "The IDS is integrated into the desired target environment and adapted to the typical data traffic. To support this, we offer a Remote Expert Assistance Service in which an SSV expert works with the user to collect the required traffic data as a CSV file via temporary read access to the OT network in order to train the embedded IDS and generate an AI model. An IDS sensor suitable for the task, e.g. a gateway, is then installed and put into operation."

The SSV Embedded IDS is available immediately either as a licensable software component or pre-installed in IDS sensor hardware. In addition to the IDET, various service dockers are also available to support automatic updates and alarm forwarding.

You will find us at SPS 2024 in hall 6 // booth 241a (Automation meets IT).

The SSV Software Systems GmbH:
SSV Software Systems was founded in Hanover in 1981 as a development service provider for microprocessor applications in logistics and automation. Since the early 1990s, the company has been developing and producing its own hardware modules and systems for industrial applications. The application focus is on industrial M2M and IoT communication. The latest developments include a product family for "fully data-based embedded system functions". Here, both the hardware CAD data and source codes for the operating system and firmware are transferred to the user to enable "deep embedded integration" into the user's own assembly. Various (I)OT/IT gateways for cyber security and wireless retrofit solutions are now being developed with the help of these technology modules.

For further questions, please contact:

SSV Software Systems GmbH
Werner Bührig
Dünenweg 5
D-30419 Hannover

E-Mail: wbu@ssv-embedded.de
Phone: +49 511 40000-22
Website: www.ssv-embedded.de
LinkedIn: www.linkedin.com/company/ssv-software-systems

You can find the corresponding images for this press release on our website www.ssv-embedded.de.

Image:

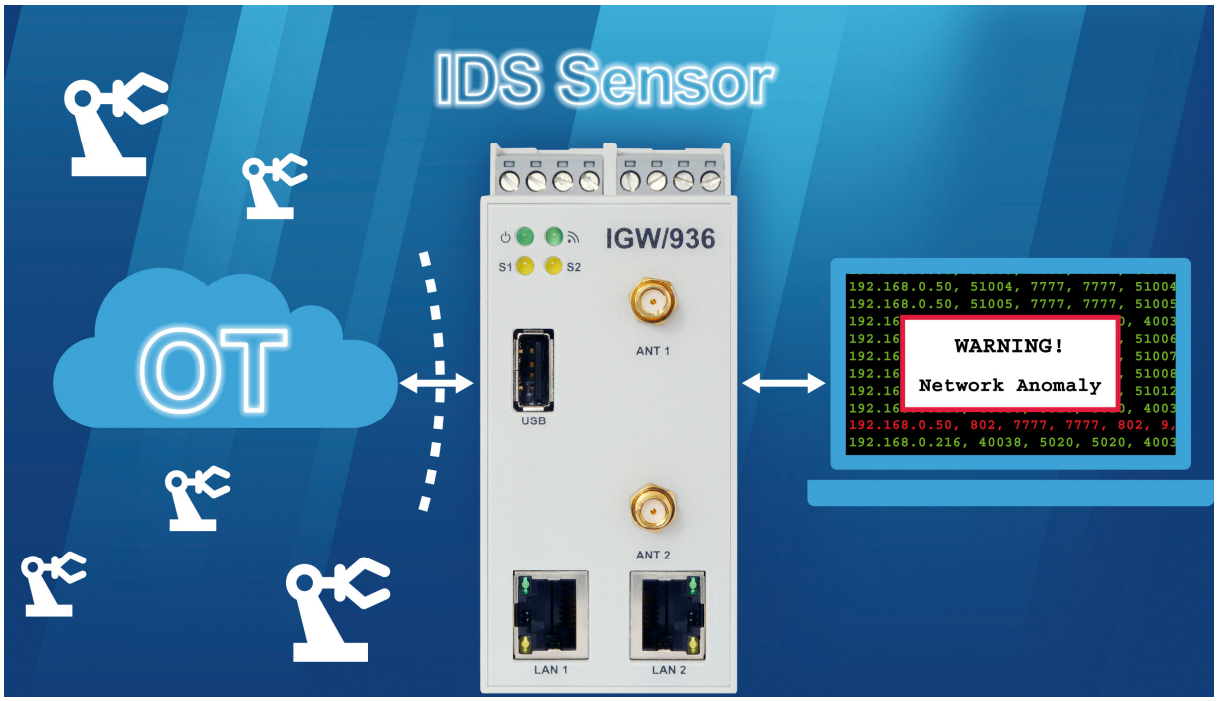

Image caption:
Networked assemblies in an Operational Technology (OT) network segment are generally weakly protected from a cyber security perspective compared to IT systems. At best, there is a firewall between the individual network segments. The OT modules themselves are relatively unprotected against cyber attacks. With the OT/IT gateway IGW/936A as an intrusion detection system (IDS) sensor, SSV offers an easy-to-use solution for automatically detecting cyber attacks and abnormal communication within OT networks. The real-time monitoring used for this is based on artificial intelligence (AI) and machine learning (ML).