Press Release

SPS 2023: OT/IT Gateway enables Virtual Patching

Due to new legal framework conditions, the Cybersecurity of Operation Technology (OT) takes on a completely new significance. In future, this will also include the obligation to remedy detected vulnerabilities through software updates. If this is not possible, a virtual patch can be realised with the IGW/936A from SSV to prevent external access to vulnerabilities in OT modules.

Hanover, September 2023. . Various new EU regulations on information technology as well as changes to product liability require a rethink with regard to OT Cybersecurity. It can be derived from these requirements that in the future, software updates for the elimination of errors and vulnerabilities will be mandatory for product providers. But the operators of IT and OT infrastructures are also challenged. They need to systematically look for and fix potential vulnerabilities with the aid of appropriate cybersecurity management processes.

In networked automation, however, there are further challenges in this regard. On the one hand, not every module within an OT network can be brought up to date by a software update if necessary. The reasons for this vary. In some cases, the manufacturers just do not develop any updates. In some cases, no current software patches are available due to End-of-support issues. In many cases, such updates are not even technically provided for or are impossible due to the construction of the components. On the other hand, there are also various functional reasons for the operators of machines and systems that speak against software updates or the replacement of certain components. These include, for example, real-time aspects, machine safety, certain contractual conditions with exclusion of liability in the event of changes, etc.

With the IGW/936A, SSV has developed a special gateway for cyber-secure OT/IT integration tasks. It is intended as an infrastructure module for domain formation or domain isolation between Ethernet-based IT networks and machines and systems. The scope of delivery includes patch management server software to activate virtual software updates in the gateway runtime environment to close the security gaps of individual OT systems. In addition, other gateway functions support secure OT/IT networking for assemblies with missing encoding, insufficient authentication as well as missing data integrity features. Via optional sensors, an IGW/936A is also suitable for additional monitoring tasks with regard to the respective application environment.

Jürgen Fitschen, the R&D manager at SSV responsible for the product concept, explains: "When designing the IGW/936A hardware and software functions, we did not only focus on access protection of the OT network interfaces, but also included access to control cabinets as well as manipulation of the environmental conditions in the parameters to be monitored via external sensors. This results in a three-dimensional cyber security approach for automation environments, with an NSL reporting interface to external alarm centres if desired."

You will find us at the SPS 2023 in hall 6 // booth 241G (Automation meets IT Area).

The SSV Software Systems GmbH:
SSV Software Systems GmbH was founded in Hanover in 1981 as a development service provider for microprocessor applications for logistics and automation. Since the early 1990s, the company has been developing and producing its own hardware assemblies and systems for industrial use. The application focus is on industrial M2M (Machine-to-machine) and IoT (Internet of Things) communication. Recent developments include complete solution modules for real-time data analysis via machine learning, full wireless sensor and network applications for predictive maintenance and condition-based monitoring. Moreover, we develop soft sensor engineering processes and remote maintenance gateways with various functions and communication interfaces.

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:

IGW/936
S1
S2
ANT 1
USB
ANT 2
LAN 1
LAN 2
IT
OT

Image caption:
Security gaps in networked modules and systems are usually closed via software updates. In networked automation, however, such a patch process for OT modules is not always possible. In some cases, updates are simply not available. Sometimes a software patch is also impossible due to plant security. In such a situation, a virtual patch for the external IGW/936A OT/IT gateway is a retrofit alternative to prevent external access to the security vulnerabilities of certain assemblies within an OT domain.