Press Release

embedded world 2022: Embedded DevOps in the Internet of Things

A construction kit with coordinated hardware and software components enables automated software delivery processes for IoT systems in order to adapt devices and applications to changing requirements during ongoing operation.

Hanover, May 2022. DevOps is a collection of different technologies and methods for organizing collaboration between software developers and application operators in terms of software maintenance. Such continuous development and maintenance processes can also be transferred to the world of embedded systems with an adapted methodology. However, in addition to the limited resources and the special interfaces, the sometimes very extreme operating environments also play a major role here. In this respect, IoT applications often involve cybersecurity maintenance (security DevOps). This requires appropriate expert knowledge and special test methods. If embedded software also contains machine learning models, an MLOps workflow is also required. It is usually used to organize the collaboration between a data science team and the application operators with regard to machine learning model maintenance.

The newly developed eDO/8331 function kit from SSV focuses on automated remote software deployment for embedded DevOps process chains. For this purpose, the kit contains a Docker-based update server, an embedded gateway DNP/8331 with an application-based Debian Linux operating system, a client software for maintainers, and PKI-based security modules. The DNP/8331 is available in a variety of mechanical formfactors ready for slot integration into user systems or as an Altium CAD function block, which license holders can embed in their own circuitry. To guarantee long-term availability for the Debian Linux operating system of the DNP/8331, SSV provides current security updates via its own repository.

With help of a development roadmap, SSV is pursuing the goal of expanding the eDO/8331 tool kit for complete IoT cyber resilience solutions. To this end, various software functions will be implemented both for the update server and the DNP/8331. These functions can protect an industrial IoT application against cyberattacks in a context-related manner, detect potential attacks based on specific behavioral patterns, and also perform automatic recovery after a cyberattack.

You will find us at the embedded world 2022 in hall 5, booth 357.

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
Tel.: +49 511 40000-22
Fax: +49 511 40000-40

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:

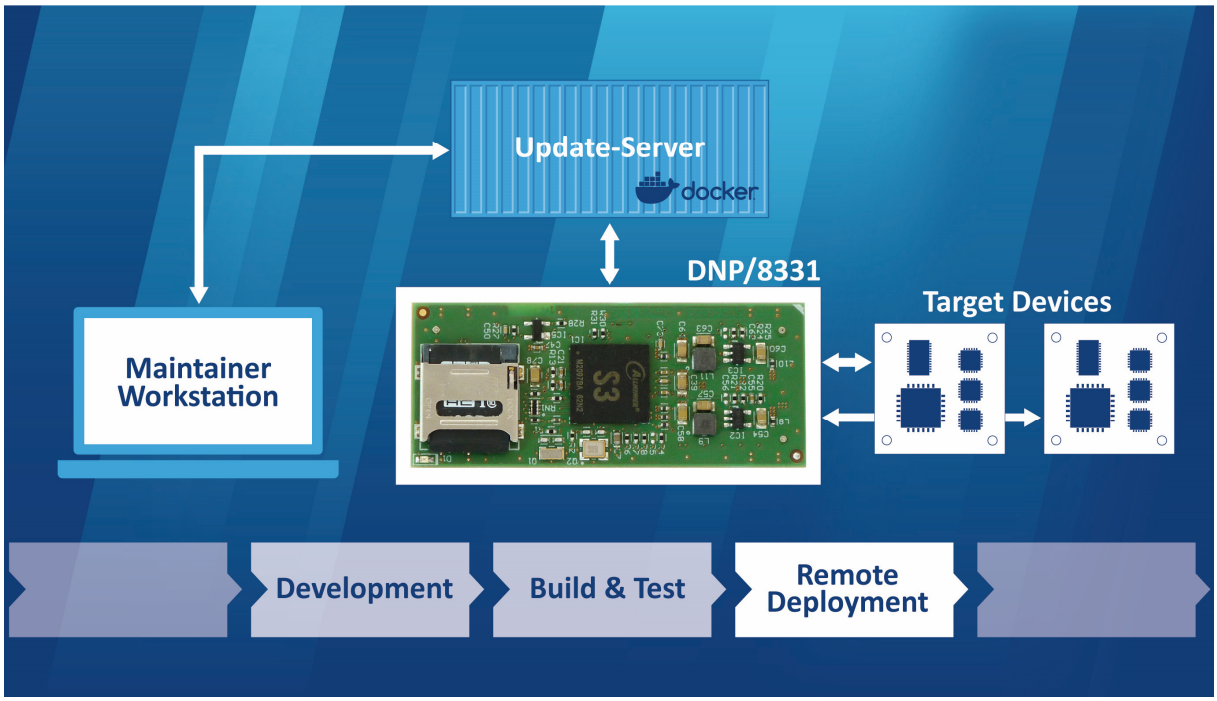

Image caption:
Software updates should be available for all functional units of an industrial IoT application via automated DevOps in order to adapt safety and functional properties to the respective requirements during its entire life cycle. For this challenge, SSV has developed the eDO/8331 function kit. It includes a Docker-based update server, an embedded gateway DNP/8331 with an application-specific Debian Linux operating system, a client software for maintainers, as well as PKI-based security modules.