PRESS RELEASE (Long Version)

CRA-compliant OTA Updates via Remote Debugger

The RED Delegated Act (RED DA) and the EU Cyber Resilience Act (CRA) create new opportunities to develop significantly higher-quality wireless IoT and embedded systems: Security by design and the ability to use software updates, for example, reduce the probability of failure. SSV's new Wireless Remote Development (WRD) Services now support developers and manufacturers in setting up a secure and long-term update pipeline to maintain user benefits throughout the entire product lifecycle.

Hanover, February 2026. The CRA stipulates that manufacturers must provide security updates as needed during the intended service life of their products in order to fix known vulnerabilities. For embedded systems, this means not only the ability to update, but also the secure, controlled, and user-friendly installation of new software versions in the field. This is exactly where SSV's WRD Services come in.

The core component is the WRD/Probe, a self-sufficient, battery-powered remote debugger with an integrated LTE-M mobile interface. It enables secure updates via SWD, JTAG, or UART interfaces. This is supplemented by GDB/GDBserver debug functions, a UART bridge, remote reset and power cycling, an integrated watchdog, telemetry data transmission, and energy monitoring for connected targets. This allows end-to-end tests to be performed directly in the real application environment – extremely helpful for proving CRA compliance. In this way, new firmware versions or edge AI modules can be comprehensively analyzed, validated, and secured directly in the field. The WRD/Probe is available in a compact housing and as an integrable module variant.

The new WRD Services also support the development of AI-based navigation solutions for mobile robots and machines. Users can, for example, develop and test Simultaneous Localization and Mapping (SLAM) methods for autonomous drones, intralogistics or cleaning robots that can orient themselves independently in unfamiliar indoor and outdoor environments while maintaining a secure radio connection to a base station.

Henrike Gerbothe, Product Manager at SSV, explains: "The WRD/Probe can now be operated in conjunction with our WRD/Box. This allows us to visualize the use of the frequency spectrum in a target environment in a task-oriented manner. This ensures, for example, that the duty cycle in an ISM band is maintained or that the listen-before-talk function of a wireless IoT sensor works as intended."

You will find us at embedded world in hall 4 // booth 602.

PRESS RELEASE (Short Version)

CRA-compliant OTA Updates via Remote Debugger

The RED Delegated Act (RED DA) and the EU Cyber Resilience Act (CRA) offer new opportunities to develop significantly higher-quality wireless IoT and embedded systems: security by design plus software updates for the entire product lifecycle increase user benefits. SSV's Wireless Remote Development (WRD) Services now provide targeted support to developers and manufacturers in setting up a secure, long-term update pipeline.

Hanover, February 2026. The CRA requirement to fix known vulnerabilities with security updates and roll them out reliably in the application requires secure, controlled, and practical update mechanisms, especially for embedded systems. With the WRD/Probe, SSV offers a self-sufficient, battery-powered remote debugger with an integrated LTE-M mobile interface. Its range of functions includes updates via SWD, JTAG, or UART interfaces as well as remote debugging, reset and power cycling, watchdog mechanisms, telemetry data transmission, and integrated energy monitoring for connected targets.

This allows new firmware versions or edge AI components to be tested and validated directly in the real application environment – including end-to-end tests to assess CRA compliance, for example. The WRD/Probe is available as a compact standalone device and as an integrable module for mobile robots and machines.

The offering is complemented by new WRD Services to support, for example, the development of AI-based navigation solutions for autonomous mobile robots while ensuring secure radio communication.

You will find us at embedded world in hall 4 // booth 602.

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, systems and solutions for industrial applications. The application focus is on industrial M2M and IoT communication as well as the development and practical use of embedded AI solutions.

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

Image:

Image caption:
Thanks to its integrated battery and LTE-M mobile interface, the WRD/Probe from SSV can be used as a self-sufficient remote debugger directly in the application environment of a wireless IoT sensor. In addition to remote debugging via SWD, JTAG, or UART interfaces, the range of functions offered by this innovative development and testing tool also includes updates, reset and power cycling, watchdog mechanisms, telemetry data transmission, and integrated energy monitoring for connected targets. WRD Services also enable remote diagnosis of an ISM frequency spectrum, for example to identify interference problems and adjust the radio software of an IoT sensor accordingly.

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