Press Release – 11 March 2026

ENFORCERS Project Launched to Strengthen European Cybersecurity Cooperation for Industrial Software and Automation

- **Cyber resilience in industry is achieved through coordinated collaboration across stakeholders**
- **ENFORCERS aims to automate the tasks of incident detection, response, certification, and secure updates**
- **Focus on strengthening industrial automation in OT environments by monitoring and tracking vulnerabilities across software supply chains**
- **The project is coordinated by WIBU-SYSTEMS AG and co-funded by the European Union**

European consortium kicks off a three-year initiative to secure software supply chains, co-ordinated incident response, and lifecycle resilience under emerging EU cybersecurity frameworks

Karlsruhe, Germany – **The European research and innovation project ENFORCERS (Enhanced Cooperation for Cybersecurity) has officially started, bringing together a strong consortium of industrial manufacturers and cybersecurity technology providers, supported by applied research organizations to address one of Europe's most pressing challenges: ensuring resilient, trustworthy software throughout the lifecycle of industrial automation systems.**

The project's official kickoff took place on 10–11 February 2026 at WIBU-SYSTEMS AG in Karlsruhe, Germany, where consortium partners met in person for the first time to align on the strategic roadmap for the coming three years. The meeting marked the operational starting point of ENFORCERS and set the stage for close cross-border collaboration enabled by EU funding.

From incident detection to secure recovery: closing the cybersecurity loop

ENFORCERS is designed to go beyond isolated security measures. Its central objective is to close the loop between cybersecurity incident detection, coordinated response, certification, and secure software redistribution in industrial environments. This is particularly relevant for automation and manufacturing, where software must often be updated across segmented, partially disconnected, or heterogeneous Operational Technology (OT) networks.

At the heart of the project is a Cybersecurity System Platform that links multiple trusted instances into a securely chained "system circle." This includes:

- **Private Security Operation Centers (SOCs)** that collect, correlate, and classify incident and vulnerability data,
- **Secure Elements** that act as trust anchors at OT edges and gateways,
- **Automated playbooks** for vulnerability mitigation, certification, and secure software updates,
- and **cross-border data exchange mechanisms** that allow SOCs and stakeholders to cooperate while respecting data sovereignty.

The technical approach directly supports compliance with **NIS2** and anticipates requirements of the **Cyber Resilience Act**, while remaining adaptable to future regulatory and technological developments.

> *"ENFORCERS brings together technologies, processes, and stakeholders into an operational cybersecurity framework," explained* ***Alvaro Forero, Project Coordinator at WIBU-SYSTEMS AG****. "As coordinator, our responsibility is to ensure that we are building a cooperative system where incident handling, trust anchors, and secure software deployment work together across organizational and national boundaries. The kickoff meeting confirmed a shared understanding that cybersecurity resilience must be engineered into the full lifecycle of industrial software."*

Clearly defined roles across a strong European consortium

ENFORCERS brings together partners with complementary expertise across Europe. As project coordinator, **Wibu-Systems** contributes its long-standing expertise in software protection, licensing, and secure update mechanisms for industrial environments, while ensuring technical coherence and cross-partner integration across the project. Industrial companies such as **Balluff (Germany and Hungary), Schneider Electric (France), TTTECH Computertechnik (Austria), and Technology Nexus Secured Business Solutions (Sweden)** contribute real-world requirements from automation, manufacturing, and industrial networking. Technology and cybersecurity specialists including **Infineon Technologies (Germany), Langlauf Security Automation (Germany), DYNAMIKI (Greece), AITAD (Germany), and ResilTech (Italy)** provide expertise ranging from AI and embedded systems to secure elements and cryptography to SOC operations and incident response. Applied research is supported by subcontractors such as **Fraunhofer SIT**, while **VDMA** contributes its industrial network and policy interface.

From a partner perspective, the project is also seen as a commitment to European cooperation.

> *"At ResilTech, we look forward to contributing with full commitment and to working alongside such high-level partners to strengthen Europe's industrial cybersecurity," said* ***Francesco Brancati, Security Solution Manager and R&D Program Manager at ResilTech Srl****, underlining the importance of cross-border collaboration as a prerequisite for resilient industrial systems.*

The project effectively integrates three essential layers of work, ranging from structural activities such as system requirements and architecture design, through practical implementation efforts including SOC integration, digital elements, and secure connectors, to quality-oriented tasks focused on dissemination, standards compliance monitoring and training.

Early milestones include the definition of legal and technical requirements, the design of the Cybersec System architecture, and the setup of initial SOC and platform components, followed by demonstrators and validation in later phases.

Industrial partners see ENFORCERS as a strategic investment in long-term resilience.

> *As **Dr. Markus Jung, VP Engineering at Balluff GmbH** emphasized during the project launch, "ENFORCERS is a great opportunity for Balluff to build a strong network with leading partners in the cybersecurity domain. The project will support us in further strengthening our cybersecurity measures and enhancing best practices across our industrial automation products, processes, and manufacturing sites. The strong consortium enables us to anticipate emerging trends in the coming years, well beyond the requirements of the Cyber Resilience Act, and ultimately helps us empower our customers to increase their own cybersecurity."*

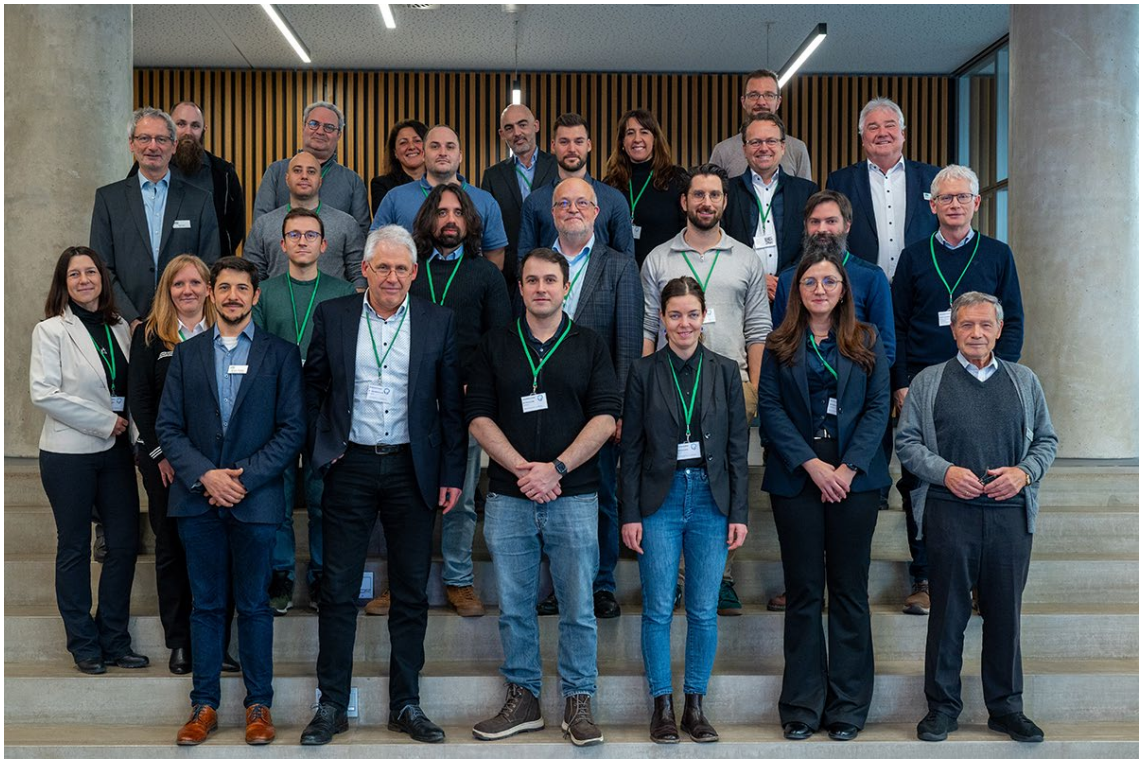
Over the next three years, ENFORCERS will deliver technical demonstrators, best practices, training activities, and contributions to standardization and certification discussions. By combining industrial deployment experience with cybersecurity expertise, the project aims to create results that are replicable across sectors and that strengthen Europe's digital sovereignty in industrial software and automation.

Co-funded by the European Union

ECCC EUROPEAN CYBERSECURITY COMPETENCE CENTRE

Co-funded by the European Union, under the Grant Agreement No. 101249745, the project is supported by the European Cybersecurity Competence Centre.

Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them.



Consortium partners at the ENFORCERS project kickoff meeting, February 2026.

Additional Dedicated Resources

- R&D project dedicated web page: https://www.wibu.com/research-and-development/enforcers.html
- Press release as audio file: https://www.wibu.com/fileadmin/Audiofiles/press_releases/WIBU-PR_ENFORCERS_EN.mp3
- Press release images for download ready for print and online publications: https://wibu.sharefile.com/public/share/web-sbab80e3b5c604ae2958f0ae407b2b739

About Wibu-Systems

Daniela Previtali, Global Marketing Director
Phone +49 721 9317235 / +39 035 0667070
daniela.previtali@wibu.com
https://www.wibu.com/

Wibu-Systems is a global leader in cutting-edge cybersecurity and software license lifecycle management. We are committed to delivering unparalleled, award-winning, and internationally patented security solutions that protect the intellectual property embedded in digital assets and amplify the monetization opportunities of technical know-how. Catering to software publishers and intelligent device manufacturers, the interoperable hardware and software modules of our comprehensive CodeMeter suite safeguard against piracy, reverse engineering, tampering, sabotage, and cyberattacks across mainstream platforms and diverse industries.

Media graphic resources available at: https://www.wibu.com/media-library.html.