

Press Release

17. Juni 2026

AUCOTEC focuses on security in engineering Cyber Security in the Focus of NIS2 and the CRA

Engineering Base software platform: proven standards for critical infrastructure – more relevant today than ever

With the NIS2 Implementation Act and the forthcoming Cyber Resilience Act (CRA), Cyber Security is currently gaining new regulatory visibility: requirements are becoming more concrete, obligations to provide evidence are increasing, and deadlines are drawing closer.

For many companies, this means: a need for action. For AUCOTEC, it means one thing above all: confirmation.

For decades, AUCOTEC has worked with operators of critical infrastructure. Throughout all these years, one central customer expectation has been taken as a given: the systems used must be secure at all times. Cyber Security is therefore not a new field of action, but has always been an integral part of the development and provision of the Engineering Base software platform.

Regulatory momentum meets established practice

The current developments surrounding NIS2 and the CRA do not change the fundamental expectation of security – they make it more visible, measurable and, in many cases, also formally subject to evidence requirements.

This is precisely where AUCOTEC creates additional transparency: Engineering Base versions 2025 and 2026 were independently analyzed using ReversingLabs Spectra Assure – and achieved Level 3 in the assessment process.

Importantly, this analysis does not mark a new security level, but confirms the one already established. At the time of the assessment, no known vulnerabilities classified as critical, no malware findings and no relevant license risks were identified. This is complemented by full transparency regarding all software components used, in the form of a Software Bill of Materials (SBOM).

External validation of an existing commitment

“Cyber Security has never been optional for our customers – and therefore not for us either,” explains Dr. Jan-Mirko Maczewski, Head of Research & Development at AUCOTEC. “Current regulatory requirements such as NIS2 or the Cyber Resilience Act are not prompting a rethink; rather, they confirm our long-standing approach.”

The Spectra analysis addresses key technical aspects of modern security requirements – in particular transparency, traceability and the systematic assessment of software components. There is no formal equivalence with regulatory requirements. However, there is substantial alignment in key areas.

For customers, this means: a robust, independent security assessment, support in meeting growing evidence requirements, reduced effort in audit and approval processes, and additional assurance in regulated project environments.

Continuity as the decisive factor

The independent assessment is deliberately designed as part of a continuous process. Security analyses are carried out regularly and continued with every version.

The fact that both the current and the already established version of Engineering Base achieve this level underlines the key message: Cyber Security at AUCOTEC is a consistent standard.

Holistically embedded – technologically and organizationally

This commitment is reflected not only in the product itself, but also in the supporting structures: ISO 27001-certified information security management, ISO 9001-certified quality management, clear responsibilities, including through a Chief Information Security Officer (CISO), as well as established audit and governance processes.

These are being continuously developed further with the ongoing expansion of Quality Excellence structures.

A clear signal in the context of new requirements

Looking ahead to the upcoming CRA deadlines and the implementation of NIS2, it is clear: Cyber Security is increasingly evolving from an implicit expectation into an explicit obligation to provide evidence. AUCOTEC is addressing this development with transparency regarding a security level that has been established for decades. Or put another way: the requirements are becoming more concrete – the response to them has long been part of the solution at AUCOTEC.



With the NIS2 Implementation Act and the upcoming Cyber Resilience Act (CRA), the topic of cybersecurity is currently gaining new regulatory visibility. (Visual: AI-generated with Adobe Firefly)



Jan-Mirko Maczewski, Head of research and Development at Aucotec (Picture: Aucotec AG)



Henry Bloch, Head of Product Management at Aucotec. (Picture: Aucotec AG)

*These images are protected by copyright. They may be used for editorial purposes in connection with AUCOTEC.

Aucotec AG develops engineering software for the entire lifecycle of machines, plants, and mobile systems – backed by more than 40 years of experience. Its solutions range from process diagrams and instrumentation and electrical engineering for large-scale plants to modular wiring systems in the automotive industry. AUCOTEC software is used worldwide. In addition to its headquarters near Hanover, the AUCOTEC Group includes six further locations in Germany as well as subsidiaries in China, India, Malaysia, South Korea, the Netherlands, France, Italy, Austria, Poland, Sweden, Norway, and the USA. A global partner network also ensures local support around the world.

If published, we kindly request a specimen copy. Thank you!

Contact:

AUCOTEC AG, Hannoversche Straße 105, 30916 Isernhagen, www.aucotec.com
Public Relations (presse@aucotec.com +49(0)511-6103192)