



Laborelec
RESEARCH & INNOVATION

CYBERSECURITY FOR INDUSTRY

Laborelec empowers organizations with a comprehensive suite of services to fortify defenses against cyber incidents.

In today's interconnected world, industrial systems are increasingly vulnerable to cyber threats. Industrial cybersecurity is crucial for safeguarding critical infrastructure, ensuring operational continuity and protecting sensitive data. Our Industrial Cybersecurity Service Suite is designed to help organizations understand the complexities of securing industrial environments and to take mitigating measures. From compliance checks and process automation projects to expert advisory services and specialized training programs, we offer comprehensive solutions to elevate the actual cybersecurity posture and protect operations from evolving threats.

For over 15 years, Laborelec has cultivated exceptional expertise in industrial cybersecurity. By collaborating with a vast network of international partners, including universities, European entities, industrial associations, and industry peers, we have developed a profound understanding of the evolving vulnerability landscape. Despite the rapid emergence of technical solutions, human factors remain one of the most critical vulnerability. Our assessments are designed to consider this reality, ensuring comprehensive protection for industrial operations.

Industrial Cybersecurity, often also indicated as OT-cybersecurity, varies from standard IT solutions, caused by the nature of industrial assets. Strict requirements to robustness and availability of process control demand protection measures that do not hamper operations in every way. Our available suite of solutions aims protecting industrial sites to the required level of resilience.

ACTIONS TO SUCCESS

Cybersecurity is fundamentally built on trust. At Laborelec, we prioritize the safe and trustworthy handling of information in all our projects. Our approach begins with a thorough understanding of your unique needs, followed by a detailed mapping against our comprehensive service suite to deliver a tailored, fit-for-purpose solution. Recognizing that each situation is distinct, we engage in a collaborative process to mutually agree on the expected deliverables.

Once the service scope is defined, we execute the work in close collaboration with your staff, ensuring seamless integration and effective implementation. Our commitment to transparency and collaboration ensures that every project is executed with precision and reliability, fostering a secure and resilient operational environment. The clear impact of our services will empower the organization to provide a proportional and effective response to its cybersecurity posture.

By leveraging our expertise and tailored solutions, you can confidently address vulnerabilities and enhance your overall security framework, ensuring robust protection against potential threats.

WHO WE WORK FOR

We serve industrial sites, primarily within Engie, committed to enhance their cybersecurity posture. Our clients include power generation facilities, storage, transmission and distribution networks, and other critical infrastructure entities. By partnering with Engie Laborelec, these organizations benefit from our extensive expertise and tailored recommendations, designed to address the unique challenges of industrial cybersecurity and safeguard their operations against evolving threats.

INTERNAL INDUSTRIAL CYBERSECURITY SERVICE SUITE INCLUDES

AUDITS / ASSESSMENTS / COMPLIANCY CHECKS / GAP ANALYSES

Ensure your current posture meets defined requirements and receive recommendations for compliance and security improvement:

- International standards (e.g., IEC62443, ISO 27k, CAF)
- NIS2 requirements
- Vulnerability Assessment
- Supplier security assessment
- Risk Management (Assessment and Methodology)
- Client's internal framework, including reporting mechanisms

CYBERSECURITY DURING PROJECTS

Evaluate the coverage of your new process automation system against project specifications:

- Employer Requirements / Tender support
- Factory Acceptance Test / Site Acceptance Test
- Cybersecurity review in design and implementation phase (Employer's Engineer)

ADVISORY SERVICES

Provide expert advice to enhance the maturity of your industrial cybersecurity implementation:

- Security architecture evaluation
- Managerial aspects recommendations
- Documentation review

TRAINING PROGRAMS

Equip your staff with specialized industrial cybersecurity knowledge:


- Awareness
- Technical staff 101 / Technical staff 102
- C-Level
- Tailor-made

WOULD YOU LIKE TO KNOW MORE?

ENGIE Laborelec

✉ storage.laborelec@engie.com

🌐 www.laborelec.com

 [Laborelec](#)

