Laborelec

Industrial control systems

Attractive targets for cyber-attacks

A five-point strategy for
a secure environment

The risk of a cyber-attack is real
… and continues to rise

Cyber threats to industrial control systems are an undeniable reality. Developments such as the Internet of Things, wireless technology, and remote access - from laptops, tablets or smartphones - heighten the risk of being hit by a cyber-attack.

A successful cyber-attack can have far-reaching consequences for your business, citizens and the environment.

Far-reaching consequences

The consequences of a successful cyber-attack should not be underestimated. First, there could be a significant impact on your business. The attack could also red-line critical parameters of your industrial control systems without your DCS and SCADA systems even noticing. By the time the sabotage is uncovered, the damage could already have been done. Recent cases have shown just how severe this damage could be, with companies often exposed to crippling financial fallout.

Legal compliance

Since cyber-attacks might also impact the environment and citizens too, many countries are working on a legislative framework to combat the phenomenon. More than ever it makes perfect sense for companies and organisations to take the issue seriously, and do everything they can to protect themselves.

Existing IT security products are impotent in the face of determined cyber-attacks.

A trusted and experienced strategic defence partner

Since existing IT security products, such as anti-virus packages and firewalls, are effectively impotent in the face of determined attacks, other solutions are urgently needed.
ENGIE Laborelec combines IT and ICS knowledge to successfully combat and prevent cyber-attacks. A five-point, end-to-end programme – from a detailed assessment of your current cyber security status to full 24/7 monitoring – safeguards your critical industrial control systems.

Examples of successful cyber-attacks

2001	• Texas, USA. DoS attack shuts down the port of Houston.
2006	• UK. Cancer treatment delayed by virus.
2007	• South Africa. Automated anti-aircraft cannon malfunctions, killing 9 people and wounding 14.
2012	• Montreal, Canada. Cascade of computer crashes causes metro system shutdown.
2014	• USA. Russian-based Dragonfly group attacks energy industry.

Source http://www.risidata.com/Database

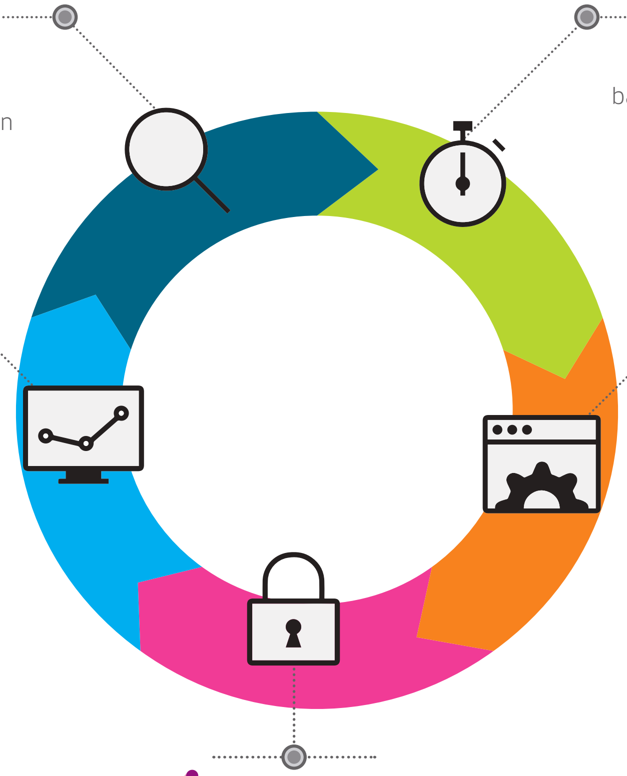
Five-point End-to-end Strategy

1 Assess

Detailed evaluation of the existing architecture, communication protocols, access rights and workflow in order to map weak spots in cyber defence.

Prioritise 2

Setting priorities, based on maximum risk reduction, balanced by cost and speed of implementation.



Remediate 3

Implementation of effective and robust measures to detect and block cyber-attacks.

4 Manage

Managing your ICS cyber security programme by monitoring key risk indicators and performing Penetration Hack Tests and operational audits to verify and improve the effectiveness of the cyber security policy.

5 Assure

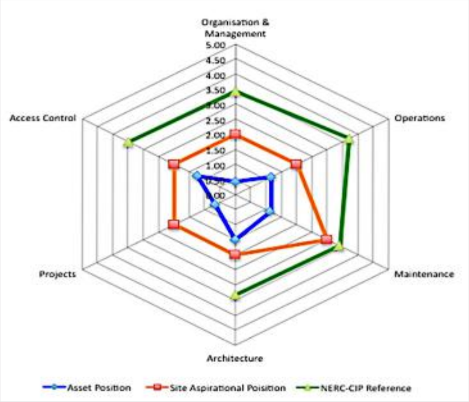
Real-time monitoring by our Secure Operations Centre, 24/7, supervised by ICS/IT specialists.

ENGIE Laborelec's **five-point security assessment strategy** will enable you to:

- Effectively communicate at all organisational levels (including management) on operational resilience against cyber threats.
- Prioritise cyber security activities and investments and develop an effective roadmap.
- Implement a cost-effective process to mitigate cyber risks.
- Apply industry best practice, international standards and local regulations.

The ENGIE Laborelec Five-point End-to-end Strategy
1 Assess & 2 Prioritise

In most cases, our five step programme starts by making a blueprint of the current security situation. Our experts map potential cyber threats and locate areas where a security breach would have the biggest impact. We can then set up a focused and well-defined plan of action to minimise the impact of cyber incidents. Moreover, we developed a training programme for the plant's personnel to increase their cyber security awareness.



The results of a 360° gap analysis are here presented in a spider chart, showing scores on six axes for the current asset position (blue), the site's aspirational position (orange) and the NERC-CIP reference (green).

ICS Cyber Security Assessment

During the ICS Cyber Security Assessment we evaluate all relevant equipment, people and processes. The assessment covers the complete life cycle, from writing the specifications, to purchasing, implementation, daily use and maintenance.

Based on a risk assessment methodology, developed in-house, we assess the criticality of individual control systems and the possible consequences of cyber-related incidents.
This enables us to map any gap between your current status and the applicable standard.

The assessment stage enables us to clearly define key performance indicators for risk, and advise where action or investment is required. Based on this information, we propose a roadmap to minimise the total cost of ownership of the cyber security improvement process. The roadmap will also be useful to local regulatory authorities.

ICS Cyber Security Awareness Training

Awareness is key in understanding the possible business impact of cyber security incidents. The main goal of this training is to provide the participants the basics of industrial control system security and learn the threats landscape.

The training is designed for process engineers, IT personnel, operations staff and other plant personnel responsible for developing and maintaining cyber security.

The ICS Cyber Security Awareness Training focuses on the basics of industrial control systems security.

The ENGIE Laborelec Five-point End-to-end Strategy
3 Remediate

This is the point at which the plan of action is brought into effect, taking into account the priorities that were set in the previous stages. It involves removing existing ineffective measures before installing a robust and effective multi-layered defence system and introducing a comprehensive training programme.

Based on a multi-layered defence strategy, we fortify your ICS environment against cyber-attacks.

Hardening solutions

We put in place a multi-layered defence strategy to block cyber-attacks, including a physical/mechanical, a software and a monitoring layer. This third layer involves the installation of monitoring tools in strategic places, enabling us to detect potential cyber-attacks from our Secure Operations Centre. The outcome is presented in a roadmap, outlining the architecture of the technical solutions and providing detailed information on the project schedule and budget.

We also set up an implementation programme – increasingly recommended by governments and regulatory authorities – which sets out the required security measures. Furthermore, we advise future steps and quick wins.

ICS Cyber Security Concepts Training

The Concepts training learns process engineers, IT personnel and plant operations staff how to defend industrial control systems against cyber threats. The training focuses on the core security principles for developing and maintaining a safe, secure and resilient operational environment. The course provides you with:

- A guidance on how to protect installations against cyber security threats
- A strategy to mitigate technical and organisational security risks
- A correct understanding and application of security policies
- Insights into strategies and protocols to secure and monitor computer networks

The training focuses on core security principles to defend industrial control systems against cyber threats.

The ENGIE Laborelec Five-point End-to-end Strategy
4 Manage & 5 Assure

Managing and improving your ICS cyber security programme requires continuous monitoring and updates. To achieve this, we monitor key risk indicators and perform Penetration Hack Tests as well as operational audits.

ENGIE Laborelec's ICS Cyber Security Penetration Hack Tests consists of a preparation phase, an onsite assessment
and a reporting phase.

ICS Cyber Security Penetration Hack Tests

Penetration Hack Tests prove that the cyber defence systems function properly and react as expected. Our tests examine both the physical and digital resilience of the targeted systems and provide a KPI for assessing and comparing individual systems. The test programme includes both unauthenticated and authenticated vulnerability and network scans, social engineering tests and a review of the technical and security settings of systems, applications and network components.

We deliver a list detailing all vulnerabilities and their potential consequences, a list of mitigation measures and an overview of (potentially) compromised systems.

ICS Secure Operations Centre

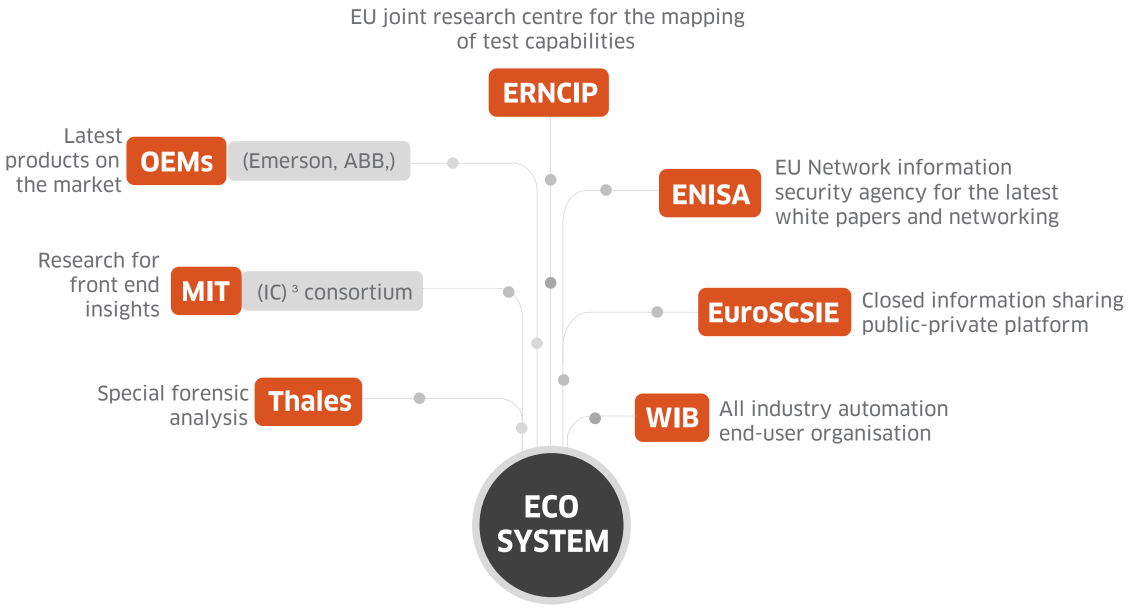
Our ICS Secure Operations Centre uses a robust, centralised monitoring solution to proactively detect and deal with cyber security issues on industrial control systems around the clock. Our experts provide Secure Remote Access services and Security Event Analysis and Forensics to guarantee secure operations of your critical automation system assets.
In case of a cyber-related issue, the Secure Operations Centre contacts you immediately and advises on mitigating actions. Subsequently, a root cause analysis is executed.

Our ICS Secure Operations Centre monitors the security of your industrial control systems around the clock.

Network & Client References

Network

We have developed an extensive ecosystem of authoritative organisations in the field of cyber security, keeping us abreast of all the latest developments and methods used by cyber criminals.



EU joint research centre for the mapping of test capabilities
ERNCIP

Latest products on the market
OEMs
(Emerson, ABB,)

EU Network information security agency for the latest white papers and networking
ENISA

Research for front end insights
MIT
(IC) ³ consortium

Closed information sharing public-private platform
EuroSCSIE

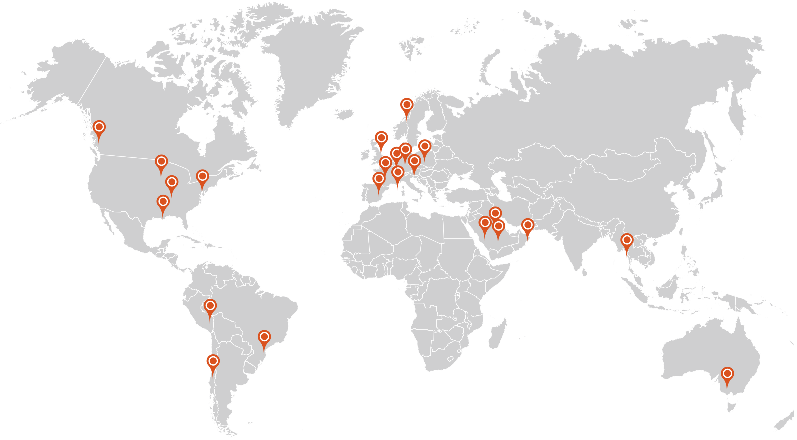
Special forensic analysis
Thales

All industry automation end-user organisation
WIB

ECO SYSTEM

Client References

We are proud to have 76 sites from different industrial branches permanently connected to our Secure Operations Centre.



The ICS Secure Operations Centre monitors

76 sites currently, in various sectors of industry worldwide

750	420	128
ASSETS	ISSL USERS	IVPN USERS

950
loglines per day

We successfully implemented a large number of cyber security projects in several domains, such as oil and gas plants, renewable power installations, nuclear and conventional power plants and power grid operators.

Why ENGIE Laborelec is your preferred partner

Combining ICS / IT expertise

Our experts are not just trained in conventional IT security, they also have vast experience in operational technology. Our knowledge of industrial control systems and industrial and energy processes, means that we speak the language of both industrial operators and IT specialists.

10 years of experience

ENGIE Laborelec's unique methodology is based on more than 10 years of hands-on experience in cyber security, international networking, and co-operation and compliance with standards institutions (NERC-CIP, WIB/IEC 62443 Vendor Requirements, ISO 27k series and others).

Multidisciplinary knowledge

ENGIE Laborelec has expertise in a wide variety of domains, giving us a clear view of the wider context in which industrial control systems function. Consequently, we have a full understanding of which parts of the industrial process are critical.

Covering the complete value chain of ICS cyber security

ENGIE Laborelec performs cyber security gap analyses, health checks and risk assessments, as well as Penetration Hack Tests and follow-up audits on governance and recoverability. We also run a Security Operation Centre for continuous round-the-clock scanning of actual security status and updating of security devices for over 76 sites currently.

Vendor-independent

ENGIE Laborelec is fully vendor-independent. Our cyber security team uses the best available tools on the market from a range of suppliers.

ENGIE
Laborelec

LABORELEC
Rodestraat 125,
1630 Linkebeek

info.laborelec@engie.com