ENGIE Laborelec and the DYNAMO Project

A Testimonial on Strengthening Cybersecurity Resilience in the Energy Sector

The DYNAMO Project: An Overview

DYNAMO is a Horizon Europe research and innovation project (responding to Cluster 3 call topic HORIZON-CL3-2021-CS-01-01) dedicated to strengthening the cyber resilience of critical infrastructure and essential service operators. It brings together a consortium of research institutions, technology developers, and end-user organisations to better prevent, respond to, and recover from cyber threats by combining business continuity management with cyber threat intelligence into a holistic resilience platform.

For the energy sector, the project is built around a simple but pressing reality: the energy sector is transforming. Traditional production facilities — coal, hydro, gas, nuclear and geothermal plants — were monolithic sites with clearly defined security perimeters, secure access control, remote locations, and lifespans exceeding 30 years. These characteristics made them relatively straightforward to defend. The newer generation of energy infrastructure — wind turbines, solar sites, micro-turbines, wave power, micro-reactors and virtual power plants — challenges those assumptions. These assets are distributed, can span enormous areas or a micro footprint, often lack a defined perimeter, require remote access, and rely on highly integrated, centrally controlled networked systems frequently embedded within urban environments.

Both approaches present significant cybersecurity challenges: balancing security against operability, budget constraints on low-margin entities, limited technical staff competence, ageing infrastructure adopting modern approaches, incomplete asset inventories, an overwhelming market of tools and vendors, the ongoing need for regulatory compliance and rapid incident detection and response and then throw in geo-political instability for fun. DYNAMO responds to these challenges by combining state-of-the-art, complementary tools that cover the full NIST Cybersecurity Framework — Identify, Protect, Detect, Respond and Recover. Rather than requiring the enormous investment of a fully in-house programme or the dependency of a purely subcontracted model, DYNAMO enables a balanced "half-half" approach: entities self-manage key aspects of their cybersecurity and grow in maturity while benefiting from trusted, industry-leading capabilities and built-in staff training.

ENGIE Laborelec's Role in the Project

Within the DYNAMO consortium, ENGIE Laborelec acts as the **End-User – Energy**. This role positions Laborelec as the voice of the energy operator, ensuring that the platform being developed reflects the real operational constraints, threat landscape and priorities of the sector.

Laborelec's most distinctive contribution is the use of its "Digital Twin" of a Gas Turbine power plant. This simulator allows the team to perform tests and simulations that would be impossible on a live, operational power plant. By connecting DYNAMO directly to this environment, Laborelec is able to validate the platform's capabilities, run realistic attack scenarios, and continuously deepen the consortium's collective knowledge through diverse use cases. Advanced attacks that could compromise a power plant and, ultimately, an operator's ability to deliver energy to its customers can be safely reproduced and studied, enabling DYNAMO to help operators respond more effectively.

Beyond the technical validation, Laborelec applies DYNAMO tools to enhance the skills of employees involved in incident response and crisis management, including training on stress management under attack conditions. Using the integrated capability of the different DYNAMO tools, the platform supports operational teams in minimising the impact of cyberattacks on energy delivery. Key to this support is improved cybersecurity awareness: helping teams better understand an attack in progress, identify which assets are likely compromised, and determine the best course of action, with Cyber Threat Intelligence (CTI) providing actionable suggestions to the incident response team.

Learnings and Experiences

Laborelec's involvement in DYNAMO has reinforced the value of testing security solutions in a realistic yet risk-free environment. The Digital Twin has proven that meaningful validation of cyber-resilience tools is possible without endangering live operations, and that simulating varied attack scenarios accelerates both platform maturity and internal expertise. Equally important has been the confirmation that technology alone is not sufficient — building the confidence, awareness and stress-resilience of the people responding to incidents is decisive in limiting the operational impact of an attack. The project has also highlighted the practical benefit of the balanced "half-half" model, allowing an energy operator to raise its cybersecurity maturity progressively, with complementary and compliant tools, rather than through disproportionate investment or full dependency on external providers. These experiences continue to shape how ENGIE Laborelec approaches the protection of an increasingly distributed and interconnected energy landscape.

For more information please visit: https://horizon-dynamo.eu/