

Project Catalogue

10 funded projects strengthening cybersecurity and resilience in the Nordic energy sector

CRESCENDO is an EU-funded initiative supporting collaborative cybersecurity projects that enhance the security, resilience of the Nordic energy sector. This catalogue presents the 10 innovative projects selected for funding.

Catalogue at a glance

Explore the 10 funded projects driving innovation and collaboration across the Nordic energy sector. Each project addresses key cybersecurity challenges and supports a more secure and resilient energy future.



10
projects

Ten innovative projects selected for funding.



Nordic
collaboration

Cross-border partnerships building knowledge and resilience.



Energy
cybersecurity

Strengthening security across the Nordic energy value chain.

Thematic overview

- 01 OT & infrastructure security**
Protecting operational technology and critical energy infrastructure.
- 02 Threat detection & testing**
Monitoring threats, identifying vulnerabilities and testing systems.
- 03 Risk & resilience**
Strengthening risk assessment, preparedness and incident response.
- 04 Secure digitalisation**
Improving security across connected devices, IT/OT integration and data flows.
- 05 Standards, regulation & compliance**
Supporting regulatory readiness, certification and practical implementation.

Cross-cutting themes: Nordic collaboration • knowledge-sharing • scalable solutions



Table of Contents

<i>Introduction</i>	<i>01</i>
<i>Map of project owners and partners</i>	<i>02</i>
<i>Himinborg – Nordic concept for resilient OT SOC's</i>	<i>03</i>
<i>Boldwark</i>	<i>04</i>
<i>Securing Battery Systems in the Nordic Energy Grid</i>	<i>05</i>
<i>AI-driven, Scenario-based Maturity Assessment for Nordic Energy Sector IT/OT Resilience</i>	<i>06</i>
<i>PORTRES – Port Energy Resilience and Security</i>	<i>07</i>
<i>Wärtsilä Secure Development Lifecycle (SDL) Certification</i>	<i>08</i>
<i>Defend the Grid: Protecting Nordic Energy SMEs Through Safe External Security Testing</i>	<i>09</i>
<i>Threat Analysis and Risk Hub 2.0</i>	<i>10</i>
<i>SecureBiz-onboard: Risk-based Authentication & Authorization for Utility Customer Onboarding and Management</i>	<i>11</i>
<i>SINERGY – Secure Integration of Neuron Sensors into Distribution Grid Systems</i>	<i>12</i>
<i>Links</i>	<i>13</i>

Introduction

CRESCENDO is pleased to present the projects selected for funding in its first call. Chosen through a competitive assessment process, the projects represent a diverse range of organisations, technologies and approaches from across the Nordic energy sector.

The projects focus on practical and scalable solutions to strengthen cybersecurity and resilience. Their activities span areas such as IT/OT security, battery energy storage systems, OT monitoring, penetration testing, risk assessment, and support for NIS2 and CER compliance.

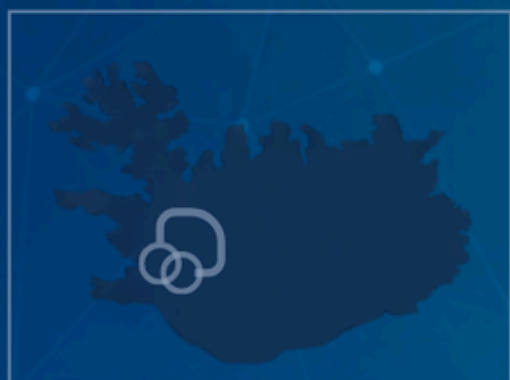
The projects will help to reduce vulnerabilities, strengthen preparedness and response capabilities, build cybersecurity expertise and support regulatory readiness. By promoting cross-border collaboration and knowledge-sharing, the projects are expected to create solutions and lessons that can be applied more widely across the Nordic energy sector.

The selected projects also highlight the breadth of the energy sector, showing that its resilience depends on a wider range of organisations, technologies and activities than might traditionally be associated with the sector.

With CRESCENDO's second funding call approaching, we hope the catalogue demonstrates the range of projects that can contribute to a more secure and resilient Nordic energy sector and encourages new organisations to take part.

Project Map

Map displaying project owners and partners for the selected projects



Himinborg – Nordic concept for resilient OT SOC^s

Project owner: NC-Spectrum AS | **Partners:** Å Energi; Glitre Nett

Keywords: *OT security; Security Operation Centres; penetration testing; scenario-based exercises*

The project addresses growing threats to the Nordic power system from hybrid attacks and increasing digital interdependencies. A key need is stronger security monitoring and response for operational technology (OT) environments.

Approach

- Develop and test a Nordic concept for resilient OT-focused Security Operations Centres (OT-SOCs).
- Assess the security and resilience of existing Security Operation Centre solutions, including technical systems, organisational structures and physical security.
- Based on this assessment, the project will develop a new OT-SOC concept and validate it through penetration testing and scenario-based exercises covering cyberattacks, hybrid threats and sabotage.
- Testing will take place in a dedicated environment to avoid disruption to critical systems.

Expected impact

The project will provide Nordic power-sector actors with a tested approach for improving their ability to detect, prevent, respond to and recover from threats to OT systems. The concept is intended for implementation within Å Energi and Glitre Nett and will also be shared more widely across the Nordic power sector.



Boldwark

Project owner: Boldwark AS | Partner: Chargerly AS

Keywords: *Embedded devices; detection and response engine; behavioural indicators*

The growing use of embedded devices such as inverters and charging units is creating new cybersecurity challenges across the energy system. These devices are increasingly deployed across distributed parts of the energy system, often with limited continuous monitoring or security controls. At the same time, the EU Cyber Resilience Act and NIS2 introduce stronger cybersecurity requirements for these devices throughout their lifecycle.

Approach

- Develop and validate a prototype embedded detection and response engine for energy-sector devices.
- Monitor device behaviour directly to identify anomalies and signs of compromise, rather than relying primarily on network traffic.
- Define behavioural indicators for normal and harmful activity and develop realistic threat scenarios.
- Test the prototype in digital twin environments replicating inverters, charging units and similar embedded energy systems.

Expected impact

The project will help manufacturers detect security incidents at device level and strengthen the resilience of embedded energy systems. Documentation and engagement with sector stakeholders will support the wider adoption of the project's results across the energy sector.



Securing Battery Systems in the Nordic Energy Grid

Project owner: Missing-Link Oy | Partners: Enetron park Oy; Koillis Lapin Sähkö Oy

Keywords: *Battery management systems; penetration testing; threat models; real-world test environments*

As battery-based power systems become increasingly connected to IT/OT environments, new cybersecurity risks are emerging across the Nordic energy grid. The project focuses on strengthening the resilience of Battery Management Systems, including risks linked to firmware and supply chains, particularly in systems using components from outside the EU.

Approach

- Conduct penetration testing to identify vulnerabilities in battery management systems and assess potential cyber-physical impacts.
- Develop threat models and cascading failure scenarios, including synchronized discharges, grid instability and transformer damage.
- Test battery systems in real-world environments, including the Honkakero battery farm and residential battery systems.
- Assess findings against relevant EU requirements, including NIS2 and CER.

Expected impact

The project will help increase the robustness of battery energy storage systems and support improved regulatory compliance. It will also produce vulnerability reports, mitigation guidelines, reusable testing protocols, threat scenario playbooks and training resources for operators, SMEs and utilities. These outputs can be used by similar organisations to strengthen cybersecurity preparedness across the wider Nordic energy sector.



AI-driven, Scenario-based Maturity Assessment for Nordic Energy Sector IT/OT Resilience

Project owner: Midlaier AS | Partners: Eidsiva Digital; SLATE – University of Bergen

Keywords: *Electricity distributors; AI-driven platform; regulatory compliance; scenario generator*

Nordic electricity distributors need to ensure that compliance with NIS2 and the Critical Entities Resilience Directive translates into effective operational risk management and incident response.

Approach

- Use an AI-driven platform to translate regulatory requirements into role-specific interview questions.
- Assess current practices and identify gaps in areas such as risk management, incident reporting and business continuity.
- Develop realistic cascading incident scenarios based on asset data and threat intelligence.
- Use scenario-based exercises to help cross-functional teams practise joint decision-making

Expected impact

The project will help energy companies strengthen crisis preparedness, improve coordination between IT, OT and risk functions, and demonstrate regulatory compliance. The resulting open-license guidance package and SaaS onboarding kit will let at least ten additional Nordic DSOs replicate the method within a year, supporting wider knowledge-sharing and operational resilience.



PORTRES – Port Energy Resilience and Security

Project owner: Defendable AS | Partners: Fjuel AS; Triple-S AS

Keywords: *Port infrastructure; secure IT/OT integrations; threat modelling; penetration testing*

Increasing digitalisation of port infrastructure is creating new cybersecurity challenges. A key challenge is the gap between IT and OT risk management, which can leave critical energy systems such as vessel charging and shore power infrastructure vulnerable to cyber threats.

Approach

- Develop and validate secure IT/OT integration frameworks for shore power systems, charging stations and local energy production.
- Conduct risk assessments, threat modelling and penetration testing to identify cybersecurity risks and vulnerabilities.
- Develop secure architectures and monitoring solutions
- Map relevant regulations and certifications for port and energy infrastructure.
- Establish a pilot environment for testing secure IT/OT integrations.

Expected impact

The project will strengthen the cyber resilience of Nordic ports and support the secure electrification of port infrastructure. It will also produce practical guidelines and scalable methods that can be applied to other ports and energy systems, such as vehicle charging infrastructure.



Wärtsilä Secure Development Lifecycle (SDL) Certification

Project owner: Wärtsilä Oyj | Partner: Sofigate Oy; Bureau Veritas Finland

Keywords: *IT/OT products; secure development practices; certification*

The project aims to strengthen the cybersecurity resilience of Wärtsilä's IT/OT products by further developing and formalising its secure development practices. A more structured Secure Development Lifecycle will help ensure that cybersecurity is systematically integrated into product development.

Approach

- Further develop Wärtsilä's Secure Development Lifecycle framework and work towards IEC 62443-4-1 certification.
- Assess existing gaps and implement targeted improvements with support from an external expert.
- Involve Wärtsilä's product development teams to ensure that the framework can be applied effectively across different real-world development environments.
- Develop and validate security-by-design practices, including threat modelling and security testing methodologies.
- Develop implementation guidance for IT/OT systems.

Expected impact

The resulting certified and scalable framework will help reduce vulnerabilities in newly developed products, strengthen cybersecurity competencies across Wärtsilä's development teams and support alignment with regulatory requirements such as NIS2 and CER.



Defend the Grid: Protecting Nordic Energy SMEs Through Safe External Security Testing 🇮🇸

Project owner: Defend Iceland ehf | Partner: Landsnet

Keywords: *Small and medium-sized energy producers; safe security testing; vetted ethical hackers*

Small and medium-sized energy producers often lack access to external security testing because it can be too costly or difficult to implement on their own. As the Nordic electricity system becomes more digital and interconnected, weaknesses in even smaller operators can have wider consequences for the energy system.

Approach

- Adapt and pilot Defend Iceland's crowdsourced cybersecurity platform in cooperation with Landsnet, Iceland's energy grid operator.
- Use vetted ethical hackers to conduct controlled external security testing and identify vulnerabilities in participating companies' systems without disrupting operations.
- Develop a safe and repeatable methodology for testing
- Translate technical findings into practical recommendations aligned with NIS2 and CER requirements.

Expected impact

The project will give participating energy producers better insight into their external attack surfaces and support more effective remediation and preparedness.



Threat Analysis and Risk Hub 2.0

Project owner: Fortified Technologies AS | Partners: Recharge News; Renergy; Ørsted

Keywords: Threat analysis; AI-supported; renewable energy; risk assessment

Rapidly evolving hybrid threats are creating a growing gap between the threat landscape and executives' ability to assess cybersecurity as a core business risk across IT and OT environments. Energy companies therefore need better tools to understand emerging threats and their potential impact at a strategic level.

Approach

- Develop Threat Analysis and Risk Hub 2.0, expanding an existing Norwegian solution to Sweden, Finland and Denmark.
- Use AI-supported analysis to identify and summarise emerging threats, actors and trends, with a focus on renewable energy sectors such as wind, solar and hydrogen.
- Develop an Executive Risk Assessment Tool covering IT/OT integration, digital supply-chain risks, organisational structures, threat intelligence and regulatory requirements including NIS2.
- Test both tools with energy companies across the Nordic region.

Expected impact

The project will give energy-sector leaders better tools for understanding and managing cybersecurity risks at a strategic level. It will also strengthen Nordic situational awareness, support regulatory compliance and help companies identify vulnerabilities across IT, OT and digital supply chains. Lessons from the Nordic pilots will support further development and potential expansion of the tools to the wider European energy sector.



SecureBiz-onboard: Risk-based Authentication & Authorization for Utility Customer Onboarding and Management 🇳🇴

Project owner: EYD AS | Partners: Allrate AS; Griter Advisory; Dun & Bradstreet Norway AS; SINTEF

Keywords: *Electricity supplier onboarding; risk assessment tool; remediation plans; threat modelling*

Onboarding new electricity suppliers can introduce new risks including the exposure of sensitive information. The project seeks to deliver a risk assessment tool to improve authentication and authorization risks and basic security for the internet/email.

Approach

- Develop a tailored risk assessment tool aligned with NIS2 and the Digital Security Act.
- Use the tool to assess more than 15 SMEs and provide tailored remediation plans.
- Develop sector benchmarks and best-practice guidance based on the assessments.
- Strengthen EYD's secure access and consent services for grid data through threat modelling, real-world onboarding scenarios and risk-based customer data.

Expected impact

The project will help electricity suppliers identify and reduce vulnerabilities, improve secure access and data protection, and strengthen regulatory readiness. Webinars, stakeholder engagement and input to the RME/Elhub working group will also support knowledge-sharing and the development of stronger access-control practices across the sector.



SINERGY – Secure Integration of Neuron Sensors into Distribution Grid Systems

Project owner: SINTEF Energi AS | Partners: Heimdal Power; Elvia; SINTEF Digital

Keywords: *Digitalisation of power systems; DSOs; real-time sensor data; SCADA systems*

The increasing digitalisation and automation of electricity distribution grids is creating new cybersecurity challenges. Distribution system operators (DSOs) increasingly depend on real-time data to maintain grid reliability and efficiency, while existing approaches to accessing high-resolution sensor data can involve cloud-based systems and manual processes that introduce delays.

Approach

- Specify and validate a secure, standards-compliant architecture for integrating real-time sensor data directly into SCADA systems.
- Define ICT and cybersecurity requirements for the integration of sensor data.
- Conduct threat modelling to identify potential cybersecurity risks.
- Carry out an operational impact analysis

Expected impact

The project will provide DSOs and regulators with a validated integration approach and supporting knowledge to reduce cybersecurity risks and accelerate the secure digitalisation of power systems, thereby contributing to more resilient electricity networks.



monitoring Al-driven role-specific onboarding regulation
supply-chain risks port management risks guidelines
penetration testing real-world environments
knowledge-sharing
IT/OT integration
cybersecurity
vulnerability reports
NIS2
secure architecture detection & response secure solutions
threat models real-world testing
Nordic energy sector

real-world impacts
cyber-physical impacts
battery systems
scenario-based testing
operation centre tools
ethical hacking training
DSOs regulatory compliance
OT IT resilience

Find us:

LinkedIn



Webpage



