ENERGY SECTOR INNOVATION PROJECTS

Guardtime has been involved in 8 EU energy sector innovation projects in the past 6 years to gain industry traction for some of our key technologies and solutions like KSI, MIDA, Alphabill, etc. Currently, we are actively involved in 2 energy projects:

- CyberSEAS - Cyber Securing Energy dAta Services
- R2D2 - Reliability, Resilience and Defence Technologies for the grid

The connections and know-how created with these six pilots in two projects can be used to generate new technology demonstrations and to create a potential basis for forming new business lines when the market needs have been validated with additional clients and stakeholders.

A short overview of these two projects is presented here. It highlights the challenges that we are solving and generalizes the status of our current work.

CyberSEAS (2021-2024)

AIM: developing cyber security tools for the protection of energy production, transmission and delivery across grids.

WHAT DO WE DO? We participate in three pilots with three large-scale grid operators from Estonia, Finland and Slovenia-Croatia to test our technologies based on the needs of the energy grid operators.

TECHNOLOGY IN ACTION: KSI, MIDA/resonance

https://cyberseas.eu «

CyberSEAS

01. Estonian pilot
partnering with Estonian energy distribution system operators (DSO) Elektrilevi and Enefit Connect.

Problem

Operational technology device firmware/-software updates come from manufacturers. These sources and repositories may not be secure. Malicious software update packages pose a threat for the whole energy grid with the result of grid shutdown.

Solution

Utilizing resonance components, we safe-guard the energy grids supply chain through a verification process where the firmware packages received from the vendors are checked when they enter Elektrilevi's system and the malicious ones (that have failed the verification) are picked out from the potential deployment process.

Status

The MIDA-based firmware update process will be tested in Elektrilevi's real environment in November 2023 and integrated into the production level, connecting it to their remote grid management system.

02. Finnish pilot
partnering with Enerim, an energy service and SaaS solutions provider in the Nordic region.

Problem

Enerim operates a service that is utilized by energy retailers and DSOs to access smart meter data and perform billing for energy consumption and production. A cyber-attacker could be able to affect the meter data or directly manipulate invoicing, with the result of causing enormous financial losses.

Solution

Resonance is used to detect the changes in metering and billing files. Data is first signed as soon as possible, and later, before bill creation or periodically, it is validated to detect any data tampering.

Status

Currently, the pilot's technical status involves defining the pilot, requirements, and solution design. The end goal of this pilot is to test and integrate our solution into Enerim's SaaS platform, enabling the provision of daily security features to 50-60% of Finland's electricity bills.

03. Slovenian - Croatian pilot
partnering with Eles, the operator of the Slovenian electric power transmission system, and HOPS, the national electricity transmission system operator in Croatia.

Problem

Currently, the high voltage energy grid model (CIM) does not have the ability to validate the data in the event of a man-in-the-middle attack or human error to ensure safe data transfer and enable safe exchange of energy from Croatia, through Slovenia, to Italy.

Solution

Resonance is utilized to enhance the security layer associated with CIM transfer and network modeling between organizations.

Status

At present, the technical status of the pilot involves defining the requirements and solution design. This information will then be used to customize and implement the solution within the Eles and HOPS test environment in November 2023.

R2D2 (2022-2025)

AIM: developing mitigation measures to improve the resilience and reliability of the energy grid.

WHAT DO WE DO? We participate in three pilots with energy distribution or transmission operators as our partners from Serbia, Greece and Slovenia.

TECHNOLOGY IN ACTION:
KSI Blockchain

https://r2d2project.eu

Contacts

For more information, please turn to project managers:

CyberSEAS

Liis Livin,
liis.livin@guardtime.com

R2D2

Mihkel Väljaots,
mihkel.valjaots@guardtime.com

01. Serbian pilot
partnering with the Serbian national transmission system operator company EMS.

Problem

EMS shares grid data with DSOs and prosumers to deliver energy to customers. This grid data and models are vulnerable to malicious tampering.

Solution

Utilizing KSI Blockchain to sign and validate exchanged data to ensure that it is not changed - an incident that could cause a major country level power outage.

Status

We are in the process of defining the requirements and solution design for this pilot. The development or the setup of the environment has not started yet. The goal is to implement our solution in EMS' test environment. The validation phase starts in second quarter of 2024 finishing in the third quarter of 2025.

02. Greek pilot
partnering with Greece's primary DSO, Hedno.

Problem

The metering data of Hedno's customers is used for billing the customers, and there is a concern about providing trusted data from metering points to the central datahub.

Solution

Resonance dockets are used to demonstrate the registration of smart meter data in the central database and provide proof when producing invoices to customers. Once the main functionality is tested and business relevance is approved, Alphabill could be introduced for future solution versions.

Status

We are in the process of defining the requirements and solution design for this pilot. The development or the setup of the environment has not started yet. The goal is to implement our solution in Hedno's test environment. The validation phase starts in the second quarter of 2024 finishes in the third quarter of 2025.

03. Slovenian pilot
partnering with Slovenian distribution system operator, Elektro-Ljubljana.

Problem

Energy consumption, production and quality data is used for business related activities and decisions by the DSO. Which makes it important for anyone to trust the data and to be sure that the provided data is authentic and has not been changed (by error, mistake or cyber-attack).

Solution

With resonance dockets, we ensure trust for the grid balancing data that DSO and other grid participants receive. We will register such data and associated metadata based on DSO's needs. Once the main functionality is tested and business relevance is approved, Alphabill could be introduced for future solution versions.

Status

We are in the process of defining the requirements and solution design for this pilot. The development or the setup of the environment has not started yet. The goal is to implement our solution in Elektro-Ljubljana's test environment. The validation phase starts in the second quarter of 2024 finishing in the third quarter of 2025.

CyberSEAS has received funding from the EU's Horizon 2020 programme and R2D2 from Horizon Europe's programme.