ITEA 3

Project Results

SecureGrid

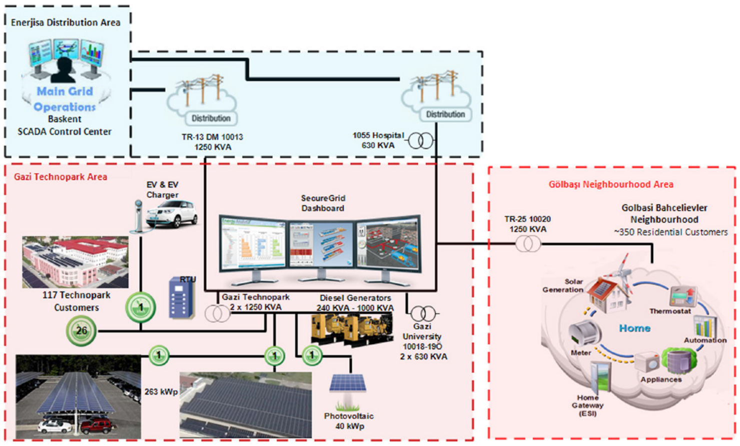
Meeting the security challenges of smart grids

EXECUTIVE SUMMARY

With a focus on smart metering, the ITEA project SecureGrid aims to provide a greater degree of power consumption management and energy fraud detection for smart grids. The Turkish-Spanish consortium achieves this through a common architecture combining AI, deep learning, business intelligence and blockchain techniques to detect and respond to attacks immediately.

PROJECT ORIGINS

The rise of smart grids should bring about cleaner electricity production, reduced energy costs, more resilient distribution and a better balance between supply and demand. Smart meters are a major enabler of these benefits – but are usually the entry point for hackers seeking to commit fraud or disrupt infrastructure. Additionally, it is impossible to push all consumers to the same brand of smart meter for their grids; interoperability between different smart metering options is therefore a necessity for realising the full potential of smart electricity management.



SecureGrid's common functional modules architecture is centred around securing the electricity grid both digitally and physically.

The SecureGrid (Security, Fraud detection and Encryption for Smart Grids based on AI) project aims to usher in a new era of energy grids. For power consumption, computational tools have been developed to analyse system and consumer data, define patterns and estimate conditions. Security is a vital component of this, so SecureGrid has developed methodologies to detect anomalies in consumption patterns based on context and previous behavioural patterns (possibly indicating fraud), as well as tools for detecting the type of intrusion. Methods are also in place to ensure the privacy and security of data transmitted by sensors and smart meters.

TECHNOLOGY APPLIED

SecureGrid's common functional modules architecture is centred around securing the electricity grid both digitally and physically and focuses on smart meters. These are found at the device layer (Home Area Network), which is connected to the system by a network layer (Neighbourhood Area Network). A business layer (Wide Area Network) contains software contributed by the consortium. On top of these three layers are separate components for data acquisition & homogenisation and persistence & quality data, which provides persistent data and improves the quality of the data received from smart meters. Other key features include business intelligence algorithms for analysis and a RESTful Application Programming Interface (API) for third-party integration and exploitation.

One of SecureGrid's most important innovations is the monitoring of large systems and the detection of abnormalities in order to prevent unexpected situations like hacking or malfunction. This is embedded in the architecture within a layer of security mechanisms & actuation techniques and features a system for detecting attacks using intelligent network techniques. This consists of four modules: Multi-Agent System, Data Pre-processing, Autoencoder and Anomaly Detection. Deep learning mechanisms are used to predict power consumption and big data analysis enables an understanding of behavioural trends, through which the system classifies all of a building's power consumption values as either normal behaviour or an attack. If behaviour changes suddenly or massively, additional deep learning algorithms can be used to detect the cause. All in all, these techniques create a more secure environment for the smart grid.

MAKING THE DIFFERENCE

SecureGrid has taken the initial steps in a relatively new domain and has demonstrated this in Ankara, where 50 to 60 different types of smart meters with different technologies (such as PLC and 5G) were installed and tested by 200 users of local facilities to indicate the interoperability of the SecureGrid platform's different technologies. Overall, Spanish partner Hermes has been able to test four million meters and it is now possible to predict energy demand with a time resolution and horizon of seven days (weekly load diagrams); a neural network model with three hidden layers and 16 neurons also allows for user categorisation with an accuracy of 80.58% (versus 76.35% for non-neural network-based algorithms). By detecting and responding to deviations from these patterns, SecureGrid will reduce the amount of money wasted on unnecessary power consumption and fraud. Through deep learning techniques, for instance, legitimate power consumption can be reduced by 70% and power consumption due to fraud can be reduced to zero.

Commercialisation is now beginning on a global scale. Hermes, for instance, has begun a pilot with a Colombian company focused on energy optimisation for medium to large industrial companies using SecureGrid's events dashboard and the fraud detection algorithm. In Turkey, meanwhile, gas distribution company IGDAS is utilising the defect/malfunction tracking components to determine regions in which malfunctions are common and take precautions. Participation in ITEA also allows the consortium partners to reach areas beyond their 'natural' markets and grow their business cases: Spanish partners can promote Turkish products to Latin America, Western Europe and West Africa whereas Turkish partners can introduce Spanish products to Eastern Europe, the Middle East and Turkic countries in Asia. This also helps consumers worldwide to benefit from smart metering.

Hopes are high for the future of SecureGrid as COVID-19 has accelerated the use of smart meters; Turkish partners in the project were involved in the management of 5000 devices prior to the pandemic but this has rapidly increased to 20,000. This trend is likely to continue, bringing with it increased opportunities for attacks. Smart grid security will therefore become increasingly relevant at a societal level, and SecureGrid provides an important foundation to realise this need.

MAJOR PROJECT OUTCOMES

Dissemination

Publications:

- OPTYFY: Industrial IoT-Based Performance and Production. Optimisation Based on Semantics.
- SEDIT: Semantic Digital Twin Based on Industrial IoT Data Management and Knowledge Graphs (5th International Conference on Technologies and Innovation, CITI 2019).

Presentations at conferences/fairs:

- International Congress of Smart Grid Solutions 2019.
- ICSG 2019: International Istanbul Smart Grid and Cities Congress.
- EUW 2019: European Utility Week.

Exploitation (so far)

New products:

- SegurAcc: verifies access to critical systems.
- CAT: attack identification by honeypots.
- SegurCom: enables fraud detection.

New services:

- SDN: allows the system to react against possible attacks to the network.

New systems:

- Mobile application for pre and post payment options: secure transaction of credits.
- Events Dashboard: visualisation of the Grid incidents at the Control Center Level.

SecureGrid
14039

Partners

Spain

Experis ManpowerGroup
Nimbeo
Sotec Consulting

Turkey

DIA Yazilim San. ve Tic. A.S.
Enerjisa Baskent Elektrik Dagitim A.S.
Ericsson Ar-Ge
Gerade Software
Kartek Kart ve Bilisim Teknolojileri Tic. A.S.

Project start
December 2017

Project end
December 2020

Project leader
Estefanía Blanco, Sotec Consulting

Project email
idi@sotec.es

Project website
https://www.securegrid-itea3.eu/