Project Outline Annex

SECUREGRID

Security, Fraud Detection and Encryption for Smart Grids based on AI

Edited by: Uc3m, Answare and contributions from all partners

Date: 31 October 2014

Apart from the State-of-the-Art-dedicated text (§2.3.1) which is handled by the ITEA Office as public information, unless otherwise specified by the consortium, this document will be treated as strictly confidential.

Project key data

Auto-generated section: input to be provided only on the Community website. Do not edit or remove this box and do not provide any text within this annex in this chapter, but provide the requested information directly on the ITEA Community website.

The inserted key data will contain (among others) the acronym, full title, time frame, the respective countries and partners per country, the coordinator, as well as a short description which should include the project idea, the main expected market impact and the main technological objective.

Table of Contents

Project key data 2

1. Project one-page description 4

2. Project overview 5

2.1. Rationale of the project 5

2.1.1. Problem statement and market value chains 5

2.1.2. Project innovations 6

2.2. Targeted impact 9

2.2.1. Market analysis 9

2.2.2. Consortium market access 15

2.2.3. Impact on quality of life 25

2.3. Technology 25

2.3.1. State-of-the-Art (SotA) analysis 25

2.3.2. Proposed technological innovation and novelty in relation to the SotA 31

2.3.3. Expected project outputs 32

2.3.4. Quantified objectives and quantification criteria 33

2.4. Consortium overview 35

2.4.1. Cooperation added value: business level 35

2.4.2. Cooperation added value: technology level 36

3. Work description 39

3.1. Project structure 39

3.2. Main milestones 41

4. Rationale for public funding (National Coordinators) 43

Annex A: Summary of costs & effort breakdown 47

1. Project one-page description

Europe is transforming the current obsolete electricity network into an advanced, digitalized and more efficient one known as smart grid. Such network incorporates the latest technologies in the field of ICT (Information and communications technology), plus advanced sensors and instrumentation systems for measuring and monitoring energy-relevant parameters. These cutting edge technologies and infrastructures provide the means to collect detailed information, which is to be served to the prosummers and processed in order to make decisions for the optimal energy production, generation, distribution, and consumption.

However, the security measures and controls developed for smart grids have not kept pace with the mentioned technical advances introduced on smart grids. For example, classical control devices and industrial instrumentation (SCADA, EMS) were not designed to provide the security required for existing smart grid systems. Despite the improvements that may introduce these systems in the network, they can also generate a large set of new controls and vulnerabilities if proper safety measures are not deployed.

Internet, light, heat, traffic control, food preservation, are just a few essential needs that require electricity to be provided. In developed countries the lack of electricity may lead to disastrous consequences as lack of food and medical supplies, monetary setbacks, loss of lives. Therefore there is no surprise in the consideration by the European Commission of the European electricity network, which serves 742.5 millions of people, as a critical infrastructure. [1]

[1] [Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection](http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008L0114:EN:HTML:NOT)

In consequence, any potential security vulnerability must be considered in order to effectively prevent, detect, and respond to them. To achieve it, the general goal of SecureGrid project is build a platform for securing Smart Grids.

One major innovative aspect of the project relies on applying AI and Big Data analysis techniques on the large amounts of data gathered by the Smart Grid. The application of these techniques is a further step that allows reasoning, gathering knowledge, planning intelligently and learning to efficiently manage security breaches.

Another innovation of the project focuses upon improving the security of the devices via the use of embedded secure elements. The challenge there is to identify low cost provisioning and deployment solutions to make the use of embedded secure elements compatible with the large deployment of possibly low cost devices deployed within a smart grid

The SecureGrid project partners have a strong commit men to developing solutions and services within the energy sector, and the consortium has been conformed in order to include companies and research centers which have proven outstanding knowledge in the main fields that the project covers: Smart Grids, Smart Metering, security, AI, Big Data.

The SecureGrid project brings together 32 partners from 6 European countries (Finland, France, The Netherlands, Portugal, Spain, and Turkey) covering the value chain for SecureGrid. In total 5 large industries, 16 SMEs, 5 research centres, 5 Universities and 1 end user.

1. Project overview
   1. Rationale of the project
      1. Problem statement and market value chains

Security requirements imposed on the data management of a smart grid are:

* Confidentiality: property for which access restrictions to information arise.
* Integrity: property that prevents the system from unauthorized modification or theft of information.
* Availability: the property for which unauthorized access is possible and prevents denial of service.
* Non-repudiation: property that prevents the execution of actions that should not be executed or the avoidance of execution of actions that should be executed.

When working with confidential information is important to know the types of attacks that can be exposed to this information in order to protect the systems involved, those are:

* Interruption: Part of the system is destroyed or unavailable.
* Interception: an unauthorized entity access to information.
* Modification: unauthorized access to information and change of its content.
* Counterfeiting: an unauthorized entity poses as a legitimate user.
* Access control and authorization management. This aspect is quite important as it addresses the problem of defining which smart grid application may interact with a device deployed in the grid and in which way

The main attacks on information systems come from the network that is the most vulnerable point for intruders. The TCP / IP protocol is not secure itself, It was designed with the objective of meeting universal access features, not security. It does not offer offers authentication, it does not keep confidentiality, and it does not have integrity.

The smart grid combines the dynamic integration of developments in electrical engineering and advances in information technology and communication in the business of electricity (generation, transmission, distribution and marketing); at the same time, using computer technology to optimize production and distribution of electricity permits to better balance supply and demand between producers and consumers. However such use of the technology together with the massiveness of the smart grid and the increased communication capabilities create potential security breaches that can affect all levels of the smart grid. Since the smart grid is considered a critical infrastructure, all vulnerabilities should be identified and sufficient solutions must be implemented to reduce the risks to an acceptable secure level.

Currently, in response to growing concerns about the current electric grid's vulnerability to cyber attacks, there is a high interest by the main stakeholders in the development of better security solutions for the Smart Grid. This is a key point since the whole energy market may be affected by any cyber-physical security attack, from the power plants to outsourcing service providers, including consumers, distribution units, etcetera.

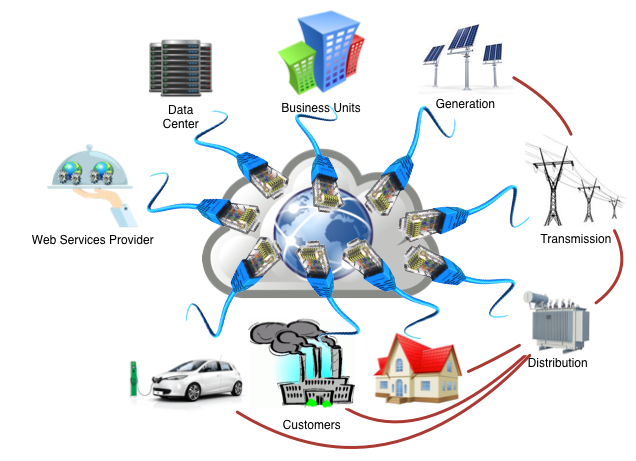


Figure 1. Energy Market Actors and Connections

The use of the Smart grid starts at the first link of the value chain: the energy production; the power plants make the production data available through the grid. Its use continues with the transportation chain, where the different meters inform about the energy circulating through the transportation means. The distribution units also submit the data about their performance via the grid. Customers make as well intensive use of the Smart grid since they use and produce data that is transmitted through the grid. Finally third outsourcing companies or other business units of the energy companies may interact with the grid by retrieving or transmitting any data. In conclusion, all the links of the energy value chain make use of the Smart grid so any of the actors of the energy market are subject to attacks.

* + 1. Project innovations

Although Smart grid is composed, in part, by tons of intelligent interconnected IT devices, **security solutions developed for traditional IT networks are not effective in grid networks** because of the major differences between them. Their security objectives -confidentiality, integrity and availability- are different from security in grid networks, which aims to provide human safety, equipment and power lines protection, and system operation [ALOUI2012]. A pack of security challenges have been identified and some broad and general solutions were proposed [KHURANA2010]; however more specific steps should be taken to bring security to the smart grid. **Big Data in Smart Grids shows plenty of advantages**, and disrupting fields of application, **but it also brings to scene some additional security issues that must be taken care of**. With this aim in mind **SecureGrid proposes several innovations to face some of these challenges**.

Big Data is intended to put together all data coming from Automated Metering Infrastructure (AMI).

From the point of view of the customer, the first application BigData help their security is **revenue protection** (in more straightforward language, theft detection) is one category seeing lots of early-stage work. AMI data can help track unbilled power [JOHN2013b].

Another core task for **customer-facing analytics** is demand response, getting customers to reduce energy consumption to reduce system peak loads [JOHN2013b] It can also focus on customer behavior, or the combination of messaging and incentives that are best at getting customers to turn down energy at a lowest possible cost to utilities.

However, using all this user related data raise a privacy issue. This is one of the reasons why Network Intrusion Prevention Systems and Network Intrusion Detection Systems technologies should enhance host-based defenses to protect the system from outside and inside attacks [ALOUI2012].

Securing communications is a system in general and in a smart grid in particular always involves two distinct phases: in a first “security bootstrap” phase initial long term credentials are being distributed. They are then usually diversified to create more ephemeral credentials used to actually protect data communications. A strong security involved the need to protect the storage of long term credentials to avoid theft of those credentials because stolen credentials may be used to impersonate the devices and provide the basis for destructive attacks. However the conception of an efficient solution to protect credential storage on an insecure device is a real challenge, and the use of secure elements embedded inside the devices constitutes a very robust solution to enhance credential storage security on the device. Secure elements may not be used standalone. Their enrolment and the management of the credentials stored in their memory are usually carried out using specialized security platforms. Traditionally those platforms are operated by the business entity which has issued the secure elements. But the need to provide end to end security in an environment where secure elements are issued by multiple actors will require delegation mechanisms to enable a trust management entity to securely provision credentials in a secure element which has been issued by another business party.

The mechanisms required for such multitenant administration of secure elements have already been started to be defined when it became necessary for Mobile telcos to enable service providers to privately administer their own credentials on a SIM card belonging to the telco. Those mechanisms may be leveraged and extended to enable the management of the credentials required for end to end security for smart grids applications.

An important challenge to facilitate the wide scale use of secure element inside smart grid devices is to keep the cost of the secure element hardware and the associated deployment costs compatible with the cost of the devices which may be very low

We hope to be able to define innovative solutions that will make possible the wide scale use of secure element even in very low cost devices, and the development of the services offered by independent trust providers. This may constitute a very significant milestone toward enhancing the security communications.

From the point of view of the network, **Outage management system** (OMS) improvements are only the most obvious way to use AMI data for operational improvements. **We’ve already seen reports of successful implementation of these** AMI-assisted outage restorations in the wake of Hurricane Sandy and other weather events. These systems could give line crews the ability to fix as-yet-unreported outages, such as those that happen when people are asleep or away from home [JOHN2013]. The next step in this line is to start diagnosing the health of grid systems themselves.

Finally, **predictive analytics** will play a key role in creating financial models that will allow utility regulators to consider the costs and benefits of future deployments Accurate demand forecasting is essential to energy planning and trading. Companies must be able to predict when they can profitably sell excess power and when they need to hedge supply [IBM2012]

Predictions are even more interesting when a applied to disaster prevention. Think of systems that can **accurately predict** where storms are expected to do their worst damage to the grid and allow utilities to stage crews and equipment accordingly. Or consider the opportunity to predict the spread of distributed generation, demand response participation and other customer-side changes to meet regulator requirements to build these expectations into future distribution grid plans, as California’s utilities are being asked to do in the next few years [JOHN2013b].

In home automation field, the Smartgrid allows user to automate their connection-disconnection of devices by enabling time-of-use pricing, but also it could be shifted to the field of personal services. Users may want to include some Personal Task Automation Rules to interact with their smart homes, e.g. turn the heating system 10 minutes before I arrive home. Here the smartphone (or maybe the car), which is not connected by default to the Smartgrid is involved, since it is providing the user's location. But as well as Hackers who compromise a meter can immediately manipulate their energy costs or fabricate generated energy meter readings [MCDANIEL2009], they can do the same with any other smart device connected to the grid. Thus, we propose an architecture where all those home automations are orchestrated though security channels and supervised by the network. Moreover, a second issue is involved, since the data used to coordinate these rules is personal and must be deleted as long as it is not needed to provide the automation of the task.

As [JOHN2013] pointed out to figure out what information that AMI network can collect from customers and deliver back to them, “You have to reach out to those customers and give them something that interests them”. In this line, home automation based in smartgrid capabilities is something that interests the user.

For the time being there is no tooling support for a complete model-driven approach that covers both safety and security issues for the utility domain. The proposed contribution led by SECUREGRID partners will be thus very innovative.

Frama-C puts a strong emphasis in providing sound analyses, in the sense that it will not report a piece of code as safe when it isn't (no false negative). Very few security analysis tools offer such guarantees (for instance, Frama-C was the only representative in the Ockham Sound Analysis category at the latest NIST SATE workshop on static analyzers for software security).

Some partners will also bring some specific technical innovation. CEA intends to promote the adoption of a model-driven approach to cover security issues in the design of complex systems. One important aspect of result evaluation will be to ease this adoption and support a system design manager in his/her certification strategy (e.g. document generation/preparation based on analysis results). In addition, CEA intends to foster the usage of formal methods for software verification in order to provide the strongest guarantees over code embedded in critical infrastructures. In order to achieve this goal, it is important to assess the tools it offers on real, industrial, case studies such as what is proposed in SECUREGRID.

[ALOUI2012] Aloul, F., Al-dalky, R., Al-mardini, M., & El-hajj, W. (2012). Smart Grid Security: Threats, Vulnerabilities and Solutions. Smart Grid and Clean Energy, (971).

[IBM2012] IBM Corporation, Managing big data for smart grids and smart meters. (2012) Available at: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=IMW14628USEN. Last visit: 22-10-2014

[JOHN2013] John, J. (2013) Making Sense of 46M Smart Meters and 1B Data Points Every Day. Available at: http://www.greentechmedia.com/articles/read/Making-Sense-of-46-Million-Smart-Meters-Delivering-1-Billion-Data-Points-Ev. Last visit: 22-10-2014

[JOHN2013b] John, J (2013) BigData on the SmartGrid : 2013 in review and 2014 Outlook. Available at:http://www.greentechmedia.com/articles/read/Big-Datas-5-Big-Steps-to-Smart-Grid-Growth-in-2014 Last visit: 22-10-2014

[KHURANA2010] Khurana, H., Hadley, M., Lu, N., &Frinke, D. A. (2010).Smart-Grid Security Issues. Security and Privacy, (February), 81–85.

[MCDANIEL2009] McDaniel, P., & McLaughlin, S. (2009). Security and Privacy Challenges in the Smart Grid. Security & Privacy, 75–77.

* 1. Targeted impact
     1. Market analysis

Our proposed phases for the market analysis are:

* Identification of exploitable results.
* Analysis of the characteristics of the market: potential market, segmentation, development and competitor analysis, even as we see this as an unique project that attacks markets with different services.
* Marketing Strategy.
* Exploitation: Business models, operational plan and operational strategies.

This exploitation must be composed of:

* Exploiting Platform: Sale of the platform within development project turnkey.
* Provision of Service (PaaS): Service system model, offering value-added services such as food service critical infrastructure or emergency systems.
* Exploitation of the applications: Operation of each of the applications separately from the platform. In some cases the proper integration will be necessary.
* Associated consulting: Creating services associated with the logical extension of the application.
* Exploitation of know-how: Exploiting the different modules in other related projects.

To carry out this plan, it will be needed a SWOT analysis of the project and an internal plan of operation in the company to a comprehensive assessment of the proposed solution. The goal is the determination and adjustment of the various dissemination activities, strategies and operational business plan provided for the project.

The goal is to obtain a final plan comprising:

* The exact and precise definition of services, including the necessary agreements with other partners to offer global solutions closed.
* The definition of the markets in which the system is intended to operate.
* The definition of sales processes associated with crossing the previous data.
* The definition of the processes of implementation and maintenance of solutions.

Smart grid security market has detected a significant increase in attacks against energy networks. North America and Asia are the first targets of these attempts and consequently the largest markets to date. However, the effective spend on Smart Grid Security to date does not proportionally follow the trend of attacks on utilities.

Annual cyber security revenue is expected to increase from $370 million to $607 million over forecast period, as it is shown in the next figure (newenergynews.blogspot.com.es/2013/04/todays-study-whats-new-on-smart-grid\_7863.html)showed). There are exceptions to prove the rule, but in general, cyber security approaches that start with grid reliability and change management appear to have been most successful.

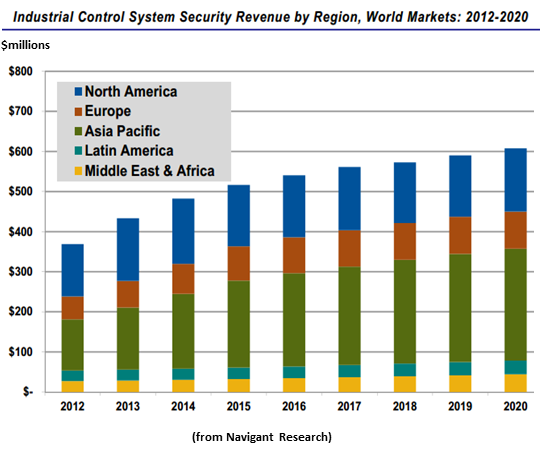


Figure 2. Industrial Control System Security Revenue by Region, World Markets: 2012-2020.

Form a security perspective, a study from beecham Research carried over the main providers of M2M solutions, identifies End to End security for communications as the most important technical challenge to be addressed (3) for the deployment of M2M/IOT communications. The importance of security is also confirmed by the increasing activity of standardization bodies (ETSI M2M, OneM2M) around this question.

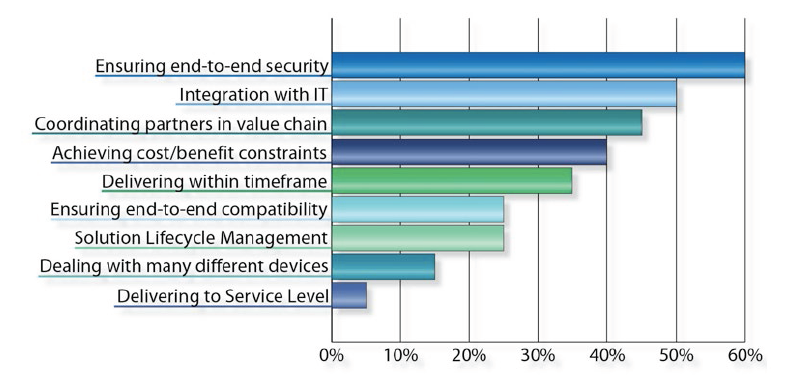
****

Figure 3 : challenges to be addressed for efficient deployment of M2M applications

End to end security implies the distribution of credentials to all end points of the communication chain, and this operation is made more complex by the fact that the parties involved in the communication schemes may not be affiliated to the same communication providers. This justifies the need for a new business actor in the ecosystem: the “Trust manager”, focused exclusively on trust management, while trust is generally managed within the framework of a specific service such as telephony or data transmission service offered by mobile network operators. This role of Trusted service manager has already appeared in the domain of mobile Financial services and more specifically NFC based services.

Also, the deployment of large scale IOT communications will require the implementation of fine grain authorization solutions to be able to define precisely which application may interact with a device and what type of interaction is authorized. The trust manager is the right actor to offer access control and authorization management services.

Also, an important challenge towards achieving strong end to end security is to address the protection of credentials stored on the device. Embedded Secure elements offer a good value proposition for this, the market is significant as the Total European market need in embedded secure elements of the energy sector for only the Energy sector is sized in tens of millions units. Lowering the personaliszation and deployment cost of embedded secure element would enlarge significantly the market size, by making the cost of secure elements compatible with the cost of low end devices which may be deployed in a smart grid.

We hope to be able to define innovative solutions that will make possible the wide scale use of secure element even in very low cost devices, and the development of the services offered by independent trust providers. This may constitute a very significant milestone toward enhancing the security of M2M/IOT communications.

**Finland:** The smart grid market is at the moment emerging in Finland after a mandatory change to smart meters in electricity has occurred. Innovations in other related fields and smart concepts such as smart cities, smart cars and smart homes have been explored. Thus, there is a good opportunity for companies with new strategies for managing the security of the new networks to gain new markets.

The Finnish consortium sees a great opportunity in this project to improve the security of the smart grids and networks both in Finland and globally. With strong participation from research and industry especially in the security and analysis fields the consortium will develop and deploy key technologies for securing the smart grids. This action is also in line with several of the main goals of the Finnish Cyber Security Strategy (http://www.defmin.fi/index.phtml?l=en&s=718), where cooperation between the government, industry actors and research partners is seen as one important factor for the success of the strategy.

**France:** The French Energy Market is characterized by a hierarchical segmentation of actors from production to transport and distribution, inherited from a long history of national monopolies, and a regulatory limitation prohibiting any incursion of DSOs in home (behind the meter). Consequently France is a bid behind north-European countries and Italy in terms of , inclusion of ICT actors in the energy value chain, with telecom operators owning the “inhome” segment where most energy-consuming equipment stand and DSOs owning the distribution grid with limited ability to enhance adaptability, load balancing, prediction and resilience. With the inherited vertical architecture of energy grids, security concerns have been traditionally addressed by way of physical network segregation, limited automations and minimal data transport. The emergence of smart grids, involving distributed and holonic architectures, active consumers, and enhanced data exchange tears down the “security by obscurity” argument. Consequently, besides debates on the effective efficiency of smart grids, a major brake to their adoption is the security issues they raise. Security of cyber-physical systems is to be seen as a “market enabler” to smarts grids, particularly in France.

Until now, Electrical network management has been centralized. Tomorrow it will be distributed and bidirectional. The main result will be a better integration of new energies and a decrease of line loss Infrastructure improvement will also enable network adaptation to new located in the French territory. In 2011, France has invested more than 180 M€ in Smart Grids projetcs among them Millener, “Bretagne d’Avance” or Premio.

The French Consortium notices that the development of secured solutions for the management of utilities networks (gas, electricity, water...)  is the best way to enable and comfort new services to end customers, without relying only on  IP-based standard communication and networks, unsecured by essence. Decentralized PV generation or Demand-Side Management requires more security and safety than the one provided by webservices as OPENADR. A secured, safe and open communication on grid services is also a path for the management of grid stability and reliability.

SECURIGRID project is considered has a way to promote secured answers at telecommunication and data management level. Having a common approach for all kind of public networks (gas, electricity, water, heat, ..) is also a way to push grid operators to share part of their dedicated telecommunication facilities, avoiding redundant investments and strengthening the resiliency of all operators through a common and coherent approach.

**Netherlands:** There have also been various initiatives started in the Netherlands on Cyber Security mainly focusing on the critical Internet and telecom infrastructures. However, the introduction of smart electricity and gas grids, as well as smart cities infrastructures are a new generation of critical infrastructures in the Netherlands. This project will bridge the gap between the methodologies from the traditional to the new generation of critical infrastructures.

**Portugal:** In Portugal the Smart Grid (SG) concepts are rapidly being transferred to the market and huge investments have already been made in renewables based electricity generation and in rolling out smart meters. Indeed, in Portugal the several investments in smart metering has led to a huge amount of consumption data that within the scope of this project will be used to extract knowledge that is crucial for the electricity regulators, grid operators and even end-users.

The Portuguese authorities from distinct fields, including the Portuguese National Communications Authority, is in line with European concerns about the urgency of working in the cyber-security communications, as the sophistication of the cyber-attacks will increase with the sophistication of the protection of the ever more complex grid operation by 2035 [“SmartGrids Strategic Research Agenda 2035”, available at www.smartgrids.eu/documents/sra2035.pd].

The Portuguese consortium has been working in smart grids topics during the last years, addressing issues such as smart grids management and resources optimization, renewable integration and forecasting, consumers profiling, demand response, etc and this project is completely in accordance with our strategy to compliment the work that has been done, the knowledge already detained and the actual infrastructures of the Portuguese grid. We highlight in particular the project outputs:

* Protection of all the systems linked to the operation, metering and end-use of electricity
* Big data analysis techniques applied on the huge amounts of data gathered to define patterns and based on that detect and prevent frauds, such as those classified as non-technical losses, but also to estimate with better accuracy the actual system considtions
* Secure communications services to ensure security and privacy of data being transmitted and gathered
* Security services and applications for the smart grid, concerning prevention, detection, impact evaluation and smart grid management according to the type of secure breaches

**Spain:** The Spanish consortium considers this project a good opportunity in the perfect time to invest in this market in Spain. The project results can be easy exploited after the right system validation and market research looking at its real possibilities and interests.

SecureGrid aims to promote future industries, fully aligned with Digital Market Services for Spain.

Key technologies such as cloud computing, the Internet of Things, the green ICT, smart markets, interoperability and applications development for the mobile ecosystem will contribute to the enrichment of the Spanish (an European) digital industry and their impact can be summarized as:

* Development and use of cloud as a key technology that will ensure the competitiveness of Spanish companies.
* Wider use of ICT that will foster energy saving.
* Better Smart Markets development and their sustainability over time.
* Major adoption of green ICT and smart grids.
* Energy savings and reduction of emissions.
* Better use of ICT infrastructure for the provision of basic services.
* Improvement of treatment methods and massive data volumes.
* Wider benefits of intelligent processing of data. Big data in organizations implies optimized decisions and improvement of productivity, efficiency and competitiveness.
* Enhancement of interoperability for a better delivery of services.

**Turkey:** Turkey has become one of the fastest growing energy markets in the world in parallel to its economic growth registered over the last ten years. The successfully implemented privatization program in the this period – power distribution is now completely in private sector hands, while the privatization of power generation assets is set to be completed within the next few years – has given the country’s energy sector a highly competitive structure and new horizons for growth. One of the latest steps the Turkish government has taken towards a more competitive energy sector, the establishment of an energy stock exchange, is in its final stage of planning. The energy stock exchange will not only enhance the liberalization of the market but will also ensure transparency and help maintain a healthy balance between supply and demand once it has become operational. Ericsson Turkey, who is already serving with software solutions to this sector plans to use the outcome of the SECUREGRID to serve this growing market.

* + 1. Consortium market access

From our point of view, the traditional approach of selling security as a compliance solution, which was successful in other industries such as finance and healthcare, leads many utilities to spend only the minimum.

Interviews for the 3Q 2012 Navigant Research report Industrial Control Systems Security (newenergynews.blogspot.com.es/2013/04/todays-study-whats-new-on-smart-grid\_7863.html) showed that cyber security vendors divide sharply into two camps:

* Control system specialists, which reported outstanding sales performance during 2012 and steady inflow of requests for proposals (RFPs).
* General-purpose security vendors, which in interviews indicated that they were not seeing much business and wondered if the market actually exists.

Next figure shows the cumulative revenue forecast from Navigant Research’s 1Q 2013 report, Smart Grid Technologies (http://www.navigantresearch.com/wp-assets/uploads/2013/03/WP-SG10T-13-Navigant-Research.pdf).

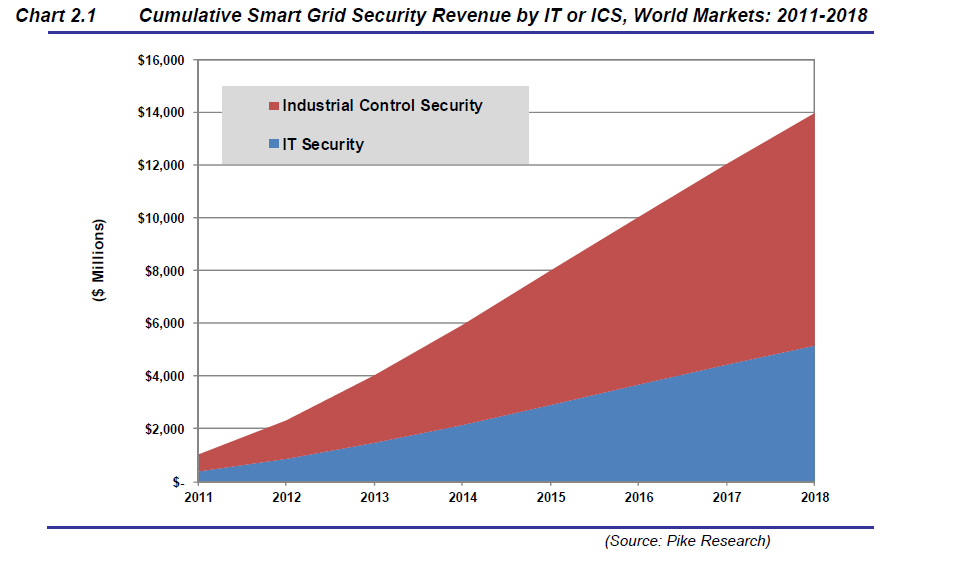


Figure 4. Cumulative Smart Grid Security Revenuew by IT or ICS, World Markets: 2011-2018.

#### Security

GlobalPlatform is a cross industry, non-profit association, which has specified over the last the last years a number of protocols for the remote management of secure elements embedded inside handset and other appliances. One of the focus of Global platform for the years to come is to make sure that the solutions they specify are applicable to secure elements embedded inside IOT devices. Some partners of this project have been involved from an early stage in the specification of the global platform protocols and will be in the position to pushnew contributions if needed to make sure that the global platform protocols are applicable to the use of embedded secure elements in smart grids appliances.

Taking into account the strong global competition, it is crucial for the European market to gain a sustainable competitive advantage. With the objective of promoting related research and development to achieve technical innovations, partners will actively act to disseminate and exploit the impact of the projects results in the European industry as well as in the scientific community.

The dissemination strategy in SecureGrids intends to build and enhance a knowledge sharing network focused on the security of smart grids’ operation that can last beyond the duration of the project, ensuring the respective follow-up by the industry and scientific communities. It intends also to influence policy-making by providing a roadmap of future initiatives on smart grids and tools for better regulation framework. Contact with previous and ongoing projects in the same area will be maintained to ensure a wider adoption of the project results as a link for further collaboration.

A set of tools including project website and communication media as well as profiles in diverse professional/social networks will assure an identity to the project in order to disseminate project results in a coherent manner. The communication strategy includes the publishing and presenting of scientific results in journals and conferences, participation in workshops and exhibitions and providing news and reports on the website and on significant social networks (LinkedIn, Facebook, Twitter).

Prototype implementations and demonstrators will be an important means of promoting project results. This will be achieved by having pilot/demonstrators in each country and by using them in exhibitions, such as ITEA 3 co-summit.

The dissemination activities will be carried out in the project according to each partner profile. Industrial partners will focus on market exploitation by disseminating the results, within its marketing activities and direct sales approaches, and by participating in industrial events, workshops and exhibitions. Academic partners will focus on scientific publications in top journals and conferences, IEEE Transactions on Industrial Informatics, Knowledge and Data Engineering, IEEE Transactions on Smart Grid, IEEE Intelligent Systems, Energy and Computer Networks (Elsevier), while research institutes will have a leading role in dissemination and organization of events that bring together research, education and industrial partners.

In the following we indicate the strategy for some partners for dissemination and exploitation plan that will be detailed in the FPP if the PO results to be successful.

|  |  |
| --- | --- |
| **Finland** | **Strategy for market access, dissemination and exploitation plans** |
| **VTT** | VTT has extensive expertise on cyber security, especially on critical infrastructure and network security. Cyber security is seen also as a great area for potential growth and improvement. VTT will develop new solutions in cooperation with the partners in SecureGrid and improve the portfolio of technologies and services that VTT can offer to its customers. |
| **Codenomicon** | The world-proven **Codenomicon** DEFENSICS platform remains unmatched in its ability to quickly find quality, resiliency and security flaws within the broadest array of applications. Thousands of developers and security analysts across telecommunications, networking, manufacturing, financial services and defense industries rely on Codenomicon to reduce costly reputation, quality and compliance risks Codenomicon brings its expertise to the project and has a keen interest in improving technologies especially in the following topics:  - robustness/reliability testing of IoT devices used in Smartgrid  - vulnerability management of embedded devices  - monitoring of IoT devices for anomalous behavior  - standardization for software reliability, safety and security |
| **nSense** | nSense's primary competences are penetration testing, vulnerability assessments of web applications and networks, and PCI DSS services. By investigating and analyzing security solutions in IT services, we help our customers test their systems and improve their level of security regardless of the deployment platform, vendor, or internal architecture. Our advisory services focus on improving information security related processes and achieving compliance with existing industry standards  The purpose of nSense attendance in the Securegrid project is to better understand the security related needs of the power and grid industry to develop security related services that directly answer the needs of the industry in question. Simultaneously nSense also makes its security related knowledge accessible to all consortium partners, to ensure secure is taken appropriately into consideration in the end product of the consortium. |
| **Indalgo** | Indalgo has extensive expertise in solving problems and creating value in various areas and applications including Manufacturing, CRM, Telecom and Context Aware solutions. Indalgo has a team of skilled data scientists that is committed to provide answers to your business questions with perfected end-to-end analytical solutions. Big data or small data, solving the question and deploying the solution to production use is the key. Indalgo will further develop their methods to tackle the challenges posed in smart grids in the SecureGrid project. |
| **University of Oulu** | In smart grids, as security challenges mainly come from malicious cyber-attacks via communication networks, it is essential to understand potential vulnerabilities in the Smart Grid under network attacks. Therefore to prevent smart grid from cyber threats or attacks, University of Oulu will focus on the following topics: Cyber security and fraud detection and contribute to the secure grid architecture design and analysis. |

|  |  |
| --- | --- |
| **France** | **Strategy for market access, dissemination and exploitation plans** |
| **CASSIDIAN** | Adapt cyber-protection and cyber-defense solution & services porfolio to the market and technical specificities of grid management. Develop cyber-physical system modelization and simulation capabilities. Enrich our security alerts with geolocalized information and provide a real time visual interface on grid security. Raise grid operators' awareness of vulnerabilities inherent to smart grids implementation and support them in scaling up security accordingly. |
| **CEA** | CEA LIST is a public research institute focusing on the development of software and hardware technology for highly integrated complex systems (transport, energy, robotics, etc). It is part of the French Alternative Energies and Atomic Energy Commission. Within LIST, the DILS department offers a wide variety of tools and techniques covering the whole software development chain, from modelling to unit, integration, and system testing. This includes in particular the design and validation of complex, critical system and software over the project life cycle, and the use of formal verification techniques on software. Tools that are particularly relevant for SECUREGRID include: - the Papyrus toolchain, an Eclipse-based open source UML-compliant software design suite - the Frama-C framework, that provide a set of analyzers for C programs (with a prototype extension to C++).  In SECUREGRID, CEA provides its expertise on safety-oriented model-driven methodology, risk-analysis and related tooling, as well as its extensive experience of large open-source software development experience (lead of Eclipse/Papyrus project) and its standardization expertise (leader of OMG MARTE profile). CEA also has experience on security-related analysis of C software through collaborative projects (STANCE and SESAM-GRIDS) and its joint lab with its spin-off TRUST-IN-SOFT. CEA also has a common laboratory with ALL4TEC (CALL4S) regarding software analysis domain. SecureGrid will provide an excellent opportunity to further develop the activity of those common laboratories and foster the technology transfer of CEA assets to ALL4TEC and TRUST-IN-SOFT.  Regarding market impact, CEA has developed various partnerships in the energy sector, through collaborative projects (CONNEXION or Sesam-Grids) or bilateral contracts. SECUREGRID will foster those partnerships by helping CEA to gear its tools towards the need of this domain.  Regarding results exploitation, CEA will extend its tools and methodologies according to the needs expressed by the SECUREGRID partners. This will result in a software offer that will be more relevant to the market needs, and can thus be more easily exploited through bilateral contracts or in the context of joint labs with software vendors such as ALL4TEC or TRUST-IN-SOFT.  Regarding dissemination, CEA will contribute based on SECUREGRID results in international conference proceedings and journals in the fields of safety assessment, security, model driven engineering, and software verification (Models, EclipseCon, LambdaMu, ESREL, ERTS, ICSE, ICST, SAS, FM, …). CEA will use its position within Eclipse and OMG to promote SECUREGRID results internationally to a wide audience. In addition, both Papyrus and Frama-C are Open Source projects and new releases will incorporate the extensions done within SECUREGRID. |
| **Citizen Data** | Citizen Data will promote securization of m2m modules and of Cloud with its WaterM plateform  Citizen Data will target- securization of m2m modules and of Cloud by approaching microgrid operator ( alliance indra , and pilot deployment with a big operator ) |
| **GDF Suez** | As project coordinator of SEAS project (semantic data exchange platform based on a knowledge model for smart energy grid), GDFSUEZ has identified cybersecurity, resilience and privacy as crucial issues for the development of decentralized energy or mobile connexion on the grid. A cooperation with another project labelled by ITEA, “MERGE Project” has been approved by the leading partners of both projects, but this cooperation doesn’t involve enough workforces to cope with the huge issues raised  by decentralized generation.  SEAS Project will give access to his field test  in order to enable the development of secured , safe and  cost-controlled answers to decentralized energy. |
| **Gemalto** | Gemalto is a leading company providing digital security solutions. We are providing solutions for protecting, verifying and managing digital identities and interactions. This enables our clients to offer personal mobile services, payment security, authenticated cloud access, identity and privacy protection, electronic documents, machine-to-machine applications and many other services.  Gemalto is creating solutions to help deploy and secure M2M applications. Our M2M portfolio is enabling applications in industries ranging from healthcare, retail services, smart energy, transportation, and logistics, automotive.  Gemalto as the world top provider of secure elements and secure element management platforms is ideally positioned to address the challenge of defining low cost secure embedded element solutions for M2M/IOT devices. Furthermore we have been involved from the beginning in the definition of the standards involved in the design and management of secure elements and this will further enhance our positioning.  Gemalto also believes in the emergence of the business role of trust manager and we intend to position as a provider of technology solutions for trust providers, but also to propose a range of trust management services to our customers deploying M2M/IOT applications.  This project is a very good opportunity for Gemalto to strengthen its position as a provider of security solutions for the utilities. Gemalto delivery will be focus on solutions embedded in smart grids devices as well as cloud secure element management platforms. The teams involved in the development of those platforms are located in the south of France |
| **Institut des Mines** | As an academic partner, IMT has no direct access to the market; however, their results obtained under the SecureGrid framework can be transferred with the view of their industrialization towards the industrial partners and towards uStartapp, a spin-off of the Institut.  The IMT actions on dissemination will be meant to rise awareness among the scientific community about the cutting-edge research aspects related to grid security in general and to confidentiality, integrity and traceability issues in particular. In this respect, the scientific publications and events organized by the IEEE, SPIE and ACM communities will be targeted. |
| **IRT SystemX** | The Research Institute of Technology SystemX (IRT SystemX) dedicated to the future system digital engineering is a powerful innovation engine for addressing the scientific and technological challenges of transport and mobility, communications, digital safety and energy markets. The involved academic and industrial Research teams large companies and SMEs) are colocated on the “Paris-Saclay Cluster” (France) and share the same ambition: strengthening the “Training-Research-Industry”momentum to generate major technology transfers and accelerate competitiveness, attractiveness and sustainability across companies and French business as a whole.  IRT SystemX will contribute to the SECUREGRID project through its own Research & Development project “EIC” (Cybersecurity Integration & Interoperability Environment) aiming to respond to complexity and growing computing safety threats of IS (information system) infrastructures thanks to a research and experimentation platform aimed for scientific and technological research around a set of capabilities, in particular:    Provide experimental reference environments :  - Access to a dedicated and configurable environment (technical, tools, infrastructure, simulators, ...)  - Representative business environments / areas: architecture, implementation and threats  - Easily reproducible and adaptable  Ability to assess the level of protection of a target environment :  - Rate security architecture for a target environment by subjecting it to specific threats to its field of activity  - Ability to integrate new safety components  In SECUREGRID Project, IRT SystemX will provide access to this platform for experimenting and evaluating fraud detection use cases in smart grids.  IRT SystemX, as an interdisciplinary thematic institute, develops the Cybersecurity economic sectors through a balanced strategic public-private partnership. For this, its EIC project contributes to the engineering of initial and continuous trainings (qualifying professional training and/or degree delivering); and ensures the exploitation of the obtained results, in particular through its large range of partner SMEs and large companies in the Cybersecurity domain. |
| **Oberthur Technologies** | OT is a Global Leader in Digital Security with a unique expertise in design & development of embedded secure software and associated solutions. As OT has established a long standing customer relationships with large and diversified customer base: +1000 financial institutions, +400 mobile operators, +100 governments OT can be seen as a Trusted M2M Partner with a dedicated organization to serve M2M customers. OT commits itself to remain a trusted and independent market player; allowing customers to avoid vendors lock-in and to simply on-board new partners.  OT is a pioneer in the M2M ecosystem, targeting a wide M2M portfolio with an end-to-end approach from connectivity management to applications enablement. OT has acquired an industrial recognition thanks to commercial deployments around the world.  What is important in the domain of smart grid is that this security is integrated in the system. Especially, a complete service shall be ensured to the subscriber. From the outputs of SECUREGRID, Oberthur would like to evangelize its customer proving the efficiency of a model based on a end 2 end security reinforced by a management system allowing openness to other services. The project will be a reference for Oberthur technology and a demonstrator for new services its can propose to its customers. |
| **University of Burgundy** | University of Burgundy will promote the results of the SecureGrid Project in the international academic community by disseminating the results and conveying the need for adopting a wise energy security management for higher education and public research centres. |
| **University of La Rochelle** | Technology Transfer and patenting when appropriate |

|  |  |
| --- | --- |
| **The NETHERLANDS** | **Strategy for market access, dissemination and exploitation plans** |
| **Target Holding and IMEC** | Although the current partners Target Holding and IMEC have a well established international business network, the Dutch consortium will be expanded after the PO phase with one or two large industrial companies to accelerate market penetration of the newly developed technologies. |

|  |  |
| --- | --- |
| **Portugal** | **Strategy for market access, dissemination and exploitation plans** |
| The Portuguese consortium is truly complementary and capable of providing solutions to integrate into the SecureGrids platform. It is a balanced mix of two SMEs, one research / academic partner and one end-user, which altogether cover the whole project scope. | |
| **Evoleo** | Evoleo provides the common framework of interaction between monitoring/controlling devices and upper data management, communication and knowledge extraction layers. As an SME, EVOLEO intends to use the outcome of this project along with others projects results to create and make available new solutions for European and Global market, through partnerships with Industry Key Players. |
| **IPBRICK** | IPBRICKwill focus on innovative solutions to provide secure communications for the smart grid. As part of the result of this project IPBRICK wants to place itself as the communications platform most adapted to build secure smart grids and will exploit the results of the SecureGrids by developing new products for system security management and fraud detection. |
| **ISEP/GECAD** | ISEP/GECAD is a research centre, within the School of Engineering of the Polytechnic of Porto, which works closely to companies in several projects and distinct areas. In this project ISEP/GECAD brings its expertise in Artificial Intelligence techniques to ensure security services and applications for the smart grid, concerning prevention, detection, impact evaluation and smart grid management according to the type of secure breaches. The results will be explored by incorporating our expertise into the companies’ solutions and thus achieving new products and services for the smart grids market. ISEP/GECAD also intends to develop consulting services and organize events, such as workshops and exhibitions, with a well balanced mix of industry, research institutes and universities. |
| **REFER** | REFERwill act as an end-user of SecureGrids solutions and the impact will be at national level as it is managing the infrastructure of the Portuguese Railway System. Indeed, this is a very critical service for a country and this first demonstration will be used to promote and exploit the project results, and at the same time will bring the Portuguese consortium the experience and skills to explore the resultant products and services on the market. REFER expects that SecureGrids results will contribute to its main objectives of supplying the market with a competitive transport infrastructure by managing and developing a safe, efficient, environment-friendly rail network, contributing to the greater use of the Railway. |

|  |  |
| --- | --- |
| **Spain** | **Strategy for market access, dissemination and exploitation plans** |
| **Answare** | Answare has a product line based on security assurance for web shopping request for any service (for example mobile device request through internet). There is a very big problem of fraud in these situations. This solution includes a Decision support system based on own technology and Big data management with Non SQL data base technologies, with time restrictions and web capabilities. SecureGrids represents a great opportunity to put our experience and efforts to support European consortium. During the life cycle of the project we will improve our technologies with the innovative developments and new techniques of SecureGrids. |
| **NIMBEO** | Nimbeo builds designs, implements and move to market high added-value tech solutions focused on EdTech, telecommunications and Smart Grids, encompassed by the Smart Big Data paradigm. This means the combination between Big Data, massive data management and Artificial Intelligence (AI), becoming a trailblazer for the Internet of Things (IoT) and making Smart Cities a reality.  Nimbeo will exploit the project by including the innovative outcomes of the project and the systems that secure the smart grid into the portfolio. Nimbeo collaborates with big players in the energy market, these players are a potential target for the exploitation of the project outcomes. Nimbeo is currently providing tools to analyse and control the smart grids; hence, the project is completely aligned with the strategy of the company. |
| **Innovati** | Innovati Servicios Tecnológicos SL is a Spanish Software Engineering SME focused on the provisioning of advanced solutions on the areas of security and human machine interaction. From just standalone apps running solutions to real complex visual frameworks or context aware software platforms, InnovatiST staff has a deep expertise into toecap technologies about user experience. Our multidisciplinary staff mixes both technicians and designers thus bringing synergies among technology and usability within our software solutions. InnovatiST staff has more than 10 years of experience in the programming field. Our software engineers have a deep technological expertise about multiplatform frameworks and tools (and therefore they are able to solutions applied to different field such as learning and social awareness). Our company provides a full set of services with high usability, security and communications requirements. It could be also highlighted that Innovati Servicios is currently partner of enerTIC (<http://www.enertic.org/>), an ICT Business Platform for improving energy efficiency. Among others, Innovati is currently collaborating with major organizations in health and learning sectors such as:  - CSIC and Hospital Doce de Octubre to facilitate rehabilitation for some chronic pathologies.  - Smartexfood, a national research project in the field of food to develop usable, accessible and context-based interfaces for the smart distribution of recommendations to improve shopping experience in supermarkets.  - Together with OEI (Organización de Estados Iberoamericanos) to deploy advanced e-learning solutions in South America.  Our main contribution in SecureGrid project will consist of the collaboration in the security, communications, usability and advanced applications.  The planned return of investment f is based on the exploitation of the technologies developed in the Project. A return ratio of 7 times is expected after 5 years exploitation.  Finally, it is important to mention that the goals of the project are perfectly aligned with this H2020 future topic (2015): DRS-12-2015: Critical Infrastructure Protection topic 1: Critical Infrastructure “smart grid” protection and resilience under “smart meters” threats (<http://ec.europa.eu/research/participants/data/ref/h2020/wp/2014_2015/main/h2020-wp1415-security_en.pdf>). |
| Universidad Politécnica de Madrid | This project represents the consolidation of a research line of the group in security management and data analysis applied to energy systems. We envision at the same time new research challenges in the consumer side of smartgrids and business opportunities to exploit results in the domain. Thus, we expect an increase of transfer capabilities of the group and also the possibility to set up a spinoff with researches involved in the project and possibly other partners of the project. In particular, the development of optimization strategies to increase the security of smart grids supported by computational methods is pointed as an outstanding contribution. |
| University of Madrid Carlos III | UC3M will promote the results of the SecureGrid Project in the international academic community by disseminating the results and conveying the need for adopting a wise energy security management for higher education and public research centres. From the dissemination and exploitation perspective, we have committed with a number of worldwide top class research institutions to apply the security algorithms, technologies and systems resulting of the SecureGrid project leveraging the smart grids already installed in both academic campus and scientific facilities which will act as the trailblazers of public intelligent energy consumption. The university is currently working with important players of the Spanish energy market on large projects related with SmarGrids such as PRICE. Hence, the university is very well related and has access to the main potential customers for the exploitation of SecureGrid |

|  |  |
| --- | --- |
| **Turkey** | **Strategy for market access, dissemination and exploitation plans** |
| **Ericsson** | Ericsson Turkey is already serving to one Electricity company in Turkey. We are already in the market and we have experienced the existing systems of regular electricity companies in business support system manners. So the results of the securegrid will be presented to Turkish electricity companies which Ericsson has already in contacted. |
| **Bor Yazılım** | Results of the project will be applied to the electric and gas distribution companies. Project results aims at increasing the efficiency of distribution companies by optimizing the maintenance and solution detection processes. Result will also enable improvement of customer service quality and customer satisfaction. |
| **Dia** | Dia is providing cloud based solutions to its enterprise customers. Based on the electricity management scenario Dia will exploit the results of the project to the energy distribution companies. |
| **Hisbim** | Turkey is security-critic country because of its geo-political position. For this reason, Turkey is really good market for final project output and good application place for prototypes. Communication and information technologies infrastructure is well built in Turkey. By this way, hi-tech prototype could be applied in Turkey without problem. Hisbim has many client out of Hisarlar in Bursa and Ankara (secondary largest industrial zones in Turkey especially in automative, aviation, defense and machinery). As you can see, Hisbim is able to access industrial market directly to implement SecureGrid system and define and apply many use-cases as use case provider SecureGrid project. |
| **Phaymobile** | Phaymobile has deep experience in mobile payment system and secure element applet development. We would like to develop end product in secure grid project for building services. We would like to integrate smart meters payment application with our existing products such as Mobile Wallet, Mobile Financial Services and our TSM products and serve a new product for our customers and market. |
| **VAS Telekom** | VAS Telekom is providing value added telecommunication services and has a customer portfolio contains business customers from different sectors. That will enable VAS Telekom to use the output of the project and knowledge gained in different sectors. |

* + 1. Impact on quality of life

In modern societies the need for a constant supply of electricity, gas and telecommunications connectivity is seen as a necessary condition for normal everyday life. Thus, it is vital to secure the smart grid against various threats that could lead into disruptions and in extreme cases to catastrophic cascading failures in the highly interconnected smart networks.

The impact of SecureGrid on the quality of life would be significant in the participating countries and also in the EU and other countries. More reliable and secure smart grids are a necessary platform for other smart concepts such as smart cars, smart cities and even e-commerce and e-government. In this sense, the project has great potential to create the fundamental prerequisites for more developed societies.

* 1. Technology
     1. State-of-the-Art (SotA) analysis

**ANN**

Artificial Neural Networks (NN) are inspired on the human brain, consisting in a huge number of neurons with high interconnectivity. A NN is constituted by a series of nodes, or neurons, organized in different levels, and interconnected by numeric weights. NNs are similar to the human brain in two essential aspects: the NN knowledge being acquired from the surrounding environment through a learning process; and the network’s nodes being interconnected by weights (synaptic weights), which are used to store the knowledge [ANN 1].

Each neuron executes a simple operation, the weighted sum of its input connections, which originates the signal that is sent to the other neurons. The network learns by adjusting the connection weights, in order to produce the desired output - the output layer values. The basic concept consists in providing the network with a large number of correct examples, so that through the comparison of the NN’s output with the correct response, it can slowly change the connection weights until it is able to generate outputs that are coincident with the correct values. This way, the NN is able to extract basic rules from real data, differing from the programmed computation, where a set of rigid and pre-defined set of rules and algorithms is necessary [ANN 2].

An NN usually presents a high accuracy in classification and forecasting, even for complex problems. Also, NNs are advantageous when dealing with redundant attributes, since the weights assigned to these attributes are usually very small. Concerning the generated outputs, NNs present the advantage of being able to originate results based on discrete values, real values, or vectors of values [ANN 3]. For this reason NNs are often applied to problems characterized by a high complexity and great variation in the problems’ data [ANN 4], such as electricity market prices forecast [ANN 1, ANN 5], load harmonics prediction [ANN 5], consumption forecasting [ANN 6], among many other.

[ANN 1] N. Amjady, A. Daraeepour, and F. Keynia, “Day-ahead electricity price forecasting by modified relief algorithm and hybrid neural network,” IET Gener. Transm. Distrib., 2010.

[ANN 2] Anbazhagan, S.; Kumarappan, N., "Day-Ahead Deregulated Electricity Market Price Forecasting Using Recurrent Neural Network," Systems Journal, IEEE , vol.7, no.4, pp.866,872, Dec. 2013.

[ANN 3] B. M. Wilamowski and H. Yu, “Neural network learning without backpropagation.,” IEEE Trans. Neural Netw., vol. 21, no. 11, pp. 1793–803, Nov. 2010.

[ANN 4] Babu, G.S.; Suresh, S., "Sequential Projection-Based Metacognitive Learning in a Radial Basis Function Network for Classification Problems," Neural Networks and Learning Systems, IEEE Transactions on , vol.24, no.2, pp.194,206, Feb. 2013.

[ANN 5] J. Mazumdar, R. G. Harley, F. C. Lambert, and G. K. Venayagamoorthy, “Neural Network Based Method for Predicting Nonlinear Load Harmonics,” IEEE Trans. Power Electron., vol. 22, no. 3, pp. 1036–1045, May 2007.

[ANN 6] Luis Hernández, Carlos Baladrón, Javier M. Aguiar, Belén Carro, Antonio Sánchez-Esguevillas, Jaime Lloret, Artificial neural networks for short-term load forecasting in microgrids environment, Energy, Volume 75, 1 October 2014, Pages 252-264, ISSN 0360-5442, http://dx.doi.org/10.1016/j.energy.2014.07.065

**SG**

The large scale integration of distributed generation, mainly based on renewable energy sources, such as photovoltaic, wind and fuel cell, is probably the biggest challenge that must be overcome in the present panorama of power systems. A globally adopted solution is approaching the electricity network as a series of subsystems, giving birth to the concept of microgrid [MG 3]. Microgrids are distributed low voltage power networks that mainly rely upon internal distributed generation units and energy storage systems for supplying their loads. They have clear electrical boundaries, being electrically connected to the power delivery system at a point of common coupling, thus appearing as a controllable single subsystem to the utility grid. In many power systems, interconnected microgrids disconnect from the grid while the system is under the stress of an abnormal condition [MG 0]. They operate in an island mode to avoid power supply interruption and eliminate possible voltage digs [MG 4]. Distribution generation units enhance the reliability of the system by providing backup generation for a microgrid during this operation mode. The small size of microgrids makes the operation more challenging, with physical implications for the performance of the power system. Load changes are large relatively to the total load, making frequency control more challenging [MG 4]. Ensuring a stable operation and security requirements during faults and various network disturbances are, thus, some of the main goals of a microgrid.

On the other hand, the main challenge of a microgrid is managing the volatility of energy generation. The power grid sees the microgrid as a single controllable entity behaving as a group of aggregated loads and generation sources [MG 1]. Lower net operating cost encourages interconnected microgrids to cooperate with each other [MG 2]. Establishing an effective coordination mechanism between microgrids and the main distribution system is a critical challenge in the short-term operation of integrated microgrids. The intelligent management and coordination of microgrids’ operation instigates the growth of the smart grid concept [SG1-SG3]. Experimental implementations of smart grids are arising all around the world [SG1, SG2], considering the management of local generation, loads, and storage systems, as independent from the main system, although connected with the main grid through a connection bus, or even working as an isolated system (in islanded mode). The intelligent management of these smaller electricity grids has been evolving and potentiating the implementation of smart grids as an upcoming reality [SG1, SG3].

[SG 1] Lund H, Andersen A, Østergaard P, Mathiesen B, Connolly D. From electricity smart grids to smart energy systems – A market operation based approach and understanding. Energy. 2012;42(1):96-102.

[SG 2] U.S. Department of Energy, “Smart Grid System Report, 2009” Available: (http://www.oe.energy.gov/)

[SG 3] Morais, H., et.al., “Multi-Level Negotiation in Smart Grids for VPP Management of Distributed Resources”, IEEE Intelligent Systems, Special Issue “Sustainable Energy and Distributed AI”, vol. 27, no. 6, pp.. 8-16, November - December 2012

[MG 0] Bo, Z., Xuesong, Z. & Jian, C. (2012). Integrated microgrid laboratory system. Power Systems, IEEE Transactions on Sower Systems, 27, 2175-2185

[MG 1] Logenthiran, T. & Srinivasan, D. (2012). Multi-agent system for the operation of an integrated microgrid. Journal of Renewable and Sustainable Energy, 4, 013116

[MG 2] Dimeas, A. L. & Hatziargyriou, N. D. (2005). Operation of a multiagent system for microgrid control. IEEE Transactions on Power Systems, 20, 1447-1455

[MG 3] Salam, A., Mohamed, A. & Hannan, M. (2008). Technical challenges on microgrids. ARPN Journal of Engineering and Applied Sciences, 3, 64-69

[MG 4] Bollen, M., Zhong, J., Samuelsson, O. & Bjornstedt, J. (2009). Performance indicators for microgrids during grid-connected and island operation. IEEE PowerTech 2009, Bucharest

**NTL**

An important concern in the power systems operation and planning is the existence of non-technical losses, also referred as commercial losses. These losses are due, for example, to the electricity theft by consumers. Unexpected load is verified in the system elements (lines, transformers, etc), making it difficult to estimate the actual system conditions, in addition to the obvious economic losses [NTL1]. These losses gain increasing importance in the competitive environment of smart grids [NTL2] since it would not be paid by regulated market roles anymore. Several works on non-technical losses’ minimization and identification have been developed [NTL3].

[NTL1] I. Monedero, F. Biscarri, C. León, J. Biscarri, and R. Millán, “Midas: Detection of non-technical losses in electrical consumption using neural networks and statistical techniques,” in Proc. Int. Conf. Comput. Sci. Appl., 2006, vol. 3984, Springer Lect. Notes Comput. Sci

[NTL2] X. Fang, S. Misra, X. Guoliang, D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," Communications Surveys & Tutorials, IEEE , vol.14, no.4, pp.944-980, Fourth Quarter 2012.

[NTL3] C.C.O. Ramos, A.N. de Souza, A.X. Falcao, J.P. Papa, "New Insights on Nontechnical Losses Characterization Through Evolutionary-Based Feature Selection," IEEE Transactions on Power Delivery, vol.27, no.1, pp.140-146, Jan. 2012

Although advances in this area have been observed in recent years, particularly with regard to the different measurement techniques of electrical energy, it becomes increasingly necessary to research alternative methods with great flexibility and easy to adaptation to the context of the problem, as computational techniques models with intelligent algorithms [NTL4].

Among the computational intelligence techniques commonly used for the detection of commercial losses are Artificial Neural Networks, Support Vector Machines, Nearest neighbors, Fuzzy Logic, among many others. The applications of these intelligent algorithms enable the development of computational tools used for the estimation and identification of fraud (commercial losses) in several companies, analyzing the data of a particular customer and their transactions, and you can check if there is any suspicious transaction occurrence of irregularity.

The intelligent techniques help to identify the potential fraudsters by analyzing data of each consumer, but the company still needs to invest in other procedures to assist in the correct identification of delinquency, as well as consumer awareness of the problem. With the aim to reduce the value of the non-technical losses, the electric energy companies usually work in:

* Inspection programs: consists in verifying the integrity of the measurement system, detecting equipment failures, fraud and theft of energy, connection errors and other problems that may compromise electrical energy measurement [NTL5];
* Replacement of meters: the assessment consisting of lots of meters through field sampling, laboratory testing and analysis of the meters removed in the field. In addition, the replacement of meters with service life expired or possible technical failures;
* Regularization of sites with high probability of illegal connections, such as slums, through a program of regulatory nature, consequently reducing commercial losses;
* Implementation of trade policies: consists of visits to the community about explanations, talks and trainings on the consumption of electricity;
* Shares of energy efficiency with a focus on reducing electric bills and effective use of energy, serving as an incentive for consumers to not defrauding.

One of the most traditional types of detect and reduce the commercial losses is conducting inspections on consumers. The selection of which consumers should be inspected is an arduous task for the experts, and then the need for the use of intelligent computational systems to help in the treatment of thousands data from millions of consumers registered.

Many actions have been taken in the search for technological solutions and methodological effective to solve the problem of trading losses. However, the experience has demonstrated the impossibility of applying unique solutions for their economic agents, even within the concession area of the business, which is due not only physical factors but mainly to the enormous cultural, social and economic society. This scenario suggests the need to construct creative solutions differentiated by the distributors.

[NTL4] R. Alves, P. Casanova, E. Quirogas, O. Ravelo, W. Gimenez, “Reduction of Non-Technical Losses by Modernization and Updating of Measurement Systems”, Transmission & Distribution Conference and Exposition: Latin America - IEEE/PES, August, 2006.

[NTL5] R. M. Queiroga, “Uso de Técnicas de Data Mining para Detecção de Fraudes em Energia Elétrica”, Dissertação de Mestrado, Universidade Federal do Espírito Santo, Vitória-ES, 2005.

**Profiling**

The characterization of electricity customers is still in progress by researches of this field of study. The spread of the measurement devices contributes to the appearance of large amounts of data relating to electricity consumption. The analysis of those data can support the definition of customer’s classes. In [P1] DM techniques are used to establish load profiles taking into account the effect of weather conditions.

For these kinds of studies, the quality of the databases is essential, as well as other additional information that can influence the electric energy consumption, such as type of activity, hired power value, consumed energy, weather conditions and tariff type [P2].

In the last years, significant research efforts have been devoted to clustering techniques in order to obtain daily load profiling [P3,P4]. In [P5] TLP are accomplished based on the Fuzzy C-Means (FCM) algorithm for consumers with hired power above 41 kW. In [P6] an original application of Support Vector Clustering (SVC) is presented for classification of electrical consumers patterns.

In [P7] an electricity consumer’s characterization study is conducted, which involved the analysis of load curves of 155 customers belonging to the medium voltage distribution systems in the north of China. This approach used three clustering algorithms: k-means, fuzzy c-means and self-organizing maps (SOM) in order to grouping the typical daily load diagrams.

[P1] Young-Il Kim, Shin-Jae Kang, Jong-Min Ko, Seung-Hwan Choi, "A study for clustering method to generate Typical Load Profiles for Smart Grid". Power Electronics and ECCE Asia (ICPE & ECCE), on IEEE 8th International Conference, May 30-June 3 2011.

[P2] S. Ramos, João Duarte, João Soares, Zita Vale, Fernando J. Duarte, "Typical Load Profiles in the Smart Grid Context – A Clustering Methods Comparison". IEEE Power and Energy Society General Meeting 2012, San Diego CA, USA, July 22 - 26 2012.

[P3] A. Mutanen, M. Ruska, S. Repo, P. Jarventausta, “Customer Classification and Load Profiling Method for Distribution Systems”. IEEE Transactions on Power Delivery, vol.26, no.3, pp.1755-1763, 2011.

[P4] M. Halkidi, Y. Batistakis, M. Vazirgiannis, "Clustering algorithms and validity measures". Tutorial paper in the proceedings of the SSDBM 2001 Conference.

[P5] D. Gerbec, S. Gasperic, I. Smon, F.Gubina, “Allocation of the load profiles to consumers using probabilistic neural networks”. IEEE Transactions on Power Systems, vol.20, no.2, pp. 548- 555, May 2005.

[P6] G. Chicco, S. Ilie, “Support Vector Clustering of Electrical Load Pattern Data”. IEEE Transactions on Power Systems, vol.24, no.3, pp.1619-1628, August 2009.

[P7] T. Zhang, G. Zhang, J. Lu, X. Feng, W. Yang, "A New Index and Classification Approach for Load Pattern Analysis of Large Electricity Customers", IEEE Transactions on Power Systems, vol.27, no.1, pp.153-160, February 2012.

Link to previous and/or current collaborative research projects:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Project Name | Cooperative Programme | Time period (approx.) | Technical Focus | Relationship |
| SEAS: Smart Energy Aware Systems | ITEA2 | Feb 2014 - Dec 2016 | SEAS addresses smart energy aware systems in building and micro-grid environments. | Cybersecurity is a concern for SEAS. SecureGrids may test and implement cyber security approaches extending SEAS platform. |
| ADAX: Attacks Detection And Countermeasures Simulation | ITEA2 | Jan 2013 - Apr 2015 | ADAX aims to study feasibility of solutions enabling to detect complex attacks against an information system working in its complex environment and to react smartly and quickly to those attacks with adapted countermeasures. | SecureGrids may extend the concepts for the electricity networks. |
| ENERFIENCY User Led Energy Efficiency Management | ITEA2 | Dec 2011 - Oct 2014 | New open platform for industrial plants, large scale buildings and citizens for the optimization of energy consumption and the definition and monitoring of business models for energy savings. | SecureGrids may extend the platform to address security vulnerabilities and how to prevent, detect and respond to them. |
| IMPONET  Intelligent Monitoring of Power Networks | ITEA2 | Dec 2010 - Mar 2013 | Research, definition, design and development of new generation IT platforms for energy management and network optimization. | SecureGrids may extend the IMPONET platform with security approaches for both remote management and monitoring. |

Table 1: Related collaborative research projects.

Some partners also have links with other projects. For example, CEA has a long history of safety and security oriented projects in various domains, among which:

* CONNEXION is an ongoing French project where CEA provides means for the safety and security analysis of large instrumentation and control infrastructure in the energy sector.
* OpenETCS is an ongoing ITEA project where safety analysis work is conducted in the railway domain
* STANCE is an ongoing FP7 project led by CEA and centered around providing analysis tools for assessing the security of C, C++ and Java programs
* SESAM-GRIDS is an ongoing French project where CEA provides tools and methods for the security analysis of smart grid components.

The experiments conducted within STANCE and SESAM-GRIDS have led to successful prototypes for software security analyzers that will be hardened and matured within SECUREGRID

* + 1. Proposed technological innovation and novelty in relation to the SotA

The potentiality of NNs to be applied to a large variety of complex problems in very distinct fields makes this technology a promising tool to approach several issues of SECUREGRIDS that require solid predicting capabilities. SECUREGRIDS will use existing NN based technologies to predict malfunctions in the grid and prevent that failures cause a high impact. Additionally, innovative, enhanced and domain directed forecasting methodologies will be proposed, based on NN derivative branches (such as Support Vector Machines, Self-Organizing Maps NN, Fuzzy Inference Systems, Deep Learning, among others).

The used and developed forecasting methodologies will also be applied to the prediction and detection of security breaches or potential attacks. Additionally, the NN based forecasting methodologies will also be used to predict the spread of distributed generation, demand response participation and other customer-side changes to meet regulators’ requirements to build these expectations into future distribution grid plans, in order to prevent problems that may arise in the future, if networks are not prepared for the expected changes.

Forecasts will provide the basis for preventive or reactive actions to be taken. These actions will be performed automatically, using machine learning methodologies to learn the best ways to act in each given context. E.g. when network faults are predicted or detected, different types of alerts must be launched depending on the gravity and impact of the failure; additionally, a network reconfiguration can be necessary, and in that case this should be defined as quickly as possible.

While characterization of consumers’ profiles has been an active area of research within the last years, in this project advances in consumers’ characterization will be used to create methodologies that automatically perceive abnormal consumption profiles, with the objective of detecting eventual cases of non-technical losses and fraud.

For power systems operation and planning the correct estimation of actual system conditions is crucial. There are several sources of uncertainties being some of them resultant from electricity theft by consumers, other resultant from the unexpected losses in the system elements, the variable production from renewable sources, the weather conditions, etc. SecureGrid will use Big Data and Artificial intelligence techniques to develop new alternative and flexible methods to estimate system actual conditions. On one hand clustering and classification will be used to define system patterns according to the context and on the other hand, based on intelligent algorithms such as Artificial Neural Networks, Support Vector Machines, Nearest Neighbours, Fuzzy Logic, among others, to estimate the actual system conditions.

There are already developments in methodologies for the intelligent management of smart grids and micro grids, usually seen as smart grids building blocks in a particular localization. These methodologies should be improved in order to accomplish the effects of distinct types of attacks and the evaluation of the specific countermeasures. This may be done by means of simulation techniques that evaluate different attacks combined with different countermeasures. In this context machine learning will improve the decision support tools by learning the effect of the attacks according to specific contexts.

While cyber-security has emerged as a very IT-focused discipline when interconnection of local networks to the internet became a standard, we acknowledge now that with the “web of objects” revolution, the “machine to machine” communication, and particularly the adoption of smart grids in the energy domain, information technology and operational (OT) technology get more and more entangled. A major limitation though is that the security of a cyber-physical system cannot just be tackled by adding physical security at OT level and cyber-security at IT level. A new federative approach is required to assess impact of cyber-incidents and countermeasures on grid operation and processes, to identify vulnerabilities of state of the art SCADA protocols in use and to identify the most likely attack scenarios in this particular environment. Therefore a particular innovation outcoming from this project will be the development of a cyber-physical system simulator to support grid security operator in assessing attack impact and selecting the most appropriate countermeasures.

One of the main novelties will be to use Big Data Analytics, machine learning and artificial intelligence on extreme large datasets for critical grid infrastructures.

* + 1. Expected project outputs

The main project result is a platform that includes a set of AI and Big Data based tools for detection, prediction and recovery of smart grids after security breaches, both concerning intrusion, confidentiality, integrity and availability.

* NN and predictive techniques to detect grid incidents, based on data and previous behavior patterns and context;
* Methodologies that detect and deal with changes in the consumption patterns claiming for possible anomalies (fraud detection, intrusion in the measurement system, etc.);
* Computational tools to analyze system and customers data, define patterns and estimate the actual system conditions (actual consumption, actual production, etc);
* Tools that based on the type of detected incidents and malfunctioning evaluate the impact on grid operation;
* Tools to manage smart grids resources according to the type of incident or malfunctioning and its impact;
* Tools for detecting any type of intrusion on the data being transmitted and gathered;
* Methods for ensuring security and privacy of data transmitted by environmental sensors and smart meters;
* Methods for ensuring security and privacy of direct load control methodologies and home automated devices;
* A decision support tool consisting mainly of a friendly interface showing the insights and the key indicators. Among others, the insights will suggest a list of actions recommended to the user based on potential risks/benefits and their impact; and the key indicators allow the users to control the most relevant measures.
* System pilots deployed in major players of the energy business in the different countries to illustrate the feasibility of SecureGrids approach in grids that are critical for country services.

The results and achievements of SecureGrid will be highly visible due to the involvement of major European large groups and in addition, they will be measurable as the pilots will take place in real plants/buildings where quantifiable comparisons will be made between the situation before and after SecureGrid.

Moreover, the achievements of SmartGrid will be implementable at short term. The system that this project will generate is an important step in the implementation of secure National/regional smart grids at mid- and long-term but it can be implemented and used well before the overall smart grid is operational. All the outcomes from this project will generate a secure smart grid, which is essential for Europe in order to protect a critical infrastructure such as the electrical network.

* + 1. Quantified objectives and quantification criteria

The market for a platform such as the one developed for SecureGrid has to be created through the demonstration of quantifiable results. SecureGrid is targeting two mains criteria which should inform the producers, consumers and third parties of the results achieved by using the SecureGrid system:

* The cost savings: by decreasing the potential attacks to the system, the costs that they generate to the stakeholders are reduced, the savings should be substantial considering the large amount of money that is floating in the energy market (a cost reduction of 2% over the amount of money earning by the energy companies is a realistic target);
* The limitation of the impact on the environment (expressed in percentage of fossil energy used and therefore in produced carbon emission) due to the protection of physical attacks that produce energy losses. This criteria is more difficult to compute, but approaching figures can be drawn out from the energy prices computed regularly from the producers as a function of the time and smart statistics).
* Defining solutions enabling wide scale adoption of embedded secure elements inside IOT appliances constitutes a formidable challenge. The use of low end IOT devices is becoming very popular, and the cost of Secure element solutions should be compatible with the cost of the devices in which they are embedded. The overall cost is split between the cost of the hardware and the cost of the deployment and configuration processes, and it is a common situation to see the cost of the process being very largely preponderant. We propose in this project to target the definition of low cost secure element solutions for IOT devices. The methodology for cost evaluation will have to be defined within the project, and according to this methodology, we believe it is reasonable goal to try to half the overall cost of the secure element.

Considering the objectives of the project, the general and specific quantification criteria are defined.

Global KPI:

* Resource management. Resource management from SecureGrid to solve any incident can be quantified according to the number of resources controlled via the platform in the 3 scenarios proposed
* Risk management. The first step in managing risk is to recognize it, scale it (measure it) and represent it using indicators. Methodologically involves the assessment of viable threats, the different aspects of vulnerability to such threats and its estimate as a situation of possible consequences of different kinds in a defined time.
* Change the trend Prevention / Solution. Exchanging the tendency to solve problems caused by attacks on smart grids for the philosophy of prevention. This criterion is measured by 10% by reducing the number of grid attacks.

Specific KPI:

* Identifying incidents. Is to gather facts, analyze them and determine if this is a known incident. 95% of incidents detection rate with a 5% of false positives per week in each scenario.
* Detect changes in consumption patterns and attempted fraud. Evaluating fraud attempt and identify the quickest ways to stop it. Fraud detection rate of 90% with a 5% false positive in a month measured in each scenario.
* Consideration of the types of incidents on the platform. Development tool that covers 100% of the types of incidents listed in the requirements analysis
* Incident management according to their type. Development tool for 100% of the types of incidents. 90% of success rate for the correct management of incidents in a week in the 3 scenarios presented.
* Detecting intrusions in the transmission of the data within the grid. The indicators are the number of intrusions and the number of detections in a month for each scenario. 98% of intrusion detection rate.
* Measuring the security and privacy of data transmitted through the grid. Percentage of incidents that have affected the confidentiality or integrity of information and time detection of incidents.
* Measuring the security and privacy of the data read directly from the automated devices. Percentage of incidents that have affected the confidentiality or integrity of information and time detection of incidents.
* The system pilots implemented. Number of system pilots deployed, number of services offered in each.

Nowadays, especially with the increasing importance of renewable electricity generation, intelligent real-time pricing system where the free market system are needed. Thus, the demand for real-time partially can be balanced and predictable renewable electricity adverse effects caused by the production on the network may be minimized. The result of all their CO2 emissions will significantly prevent, environment be said to be friendly technology. For instance by General Electric 10% of homes in the United States 3,724,197 tons of CO2 through the use of smart meters release is blocked. When this rate of over 9 million tons of emissions to be 25% will be prevented. Smart grid communications infrastructure with real-time overload could feel the energy flow to regulate aspects of renewable energy sources will pull down user costs and optimizing the use of an environmentalist will create a system in Europe in this project, then this knowledge will be distributed to all over world.

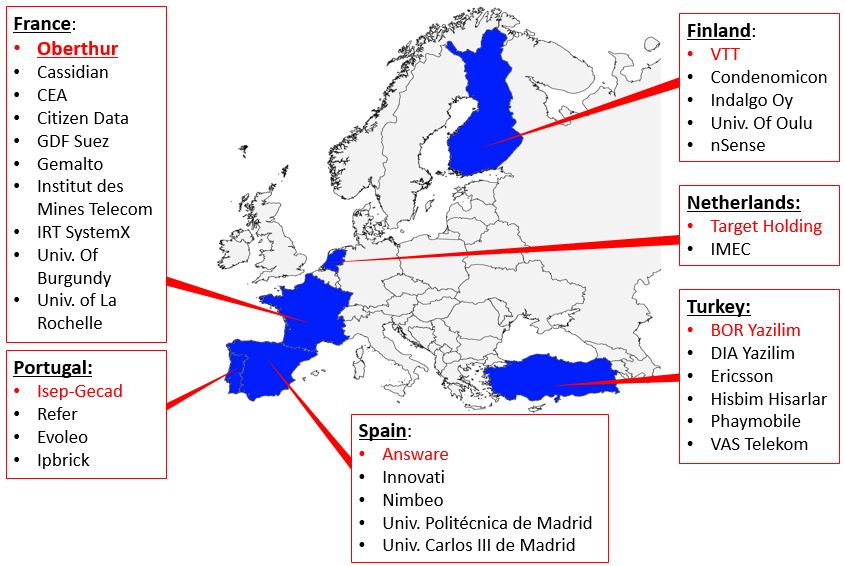
* 1. Consortium overview
     1. Cooperation added value: business level

To build up a credible consortium, the strategy has been to assemble a team of industrial and research players with extensive experience in the field of security and grids at national and international level. SecureGrid brings together a complementary pool of experts in their technological field as well as an end user to demonstrate the concept.

The SecureGrid project brings together 32 partners from 6 European countries (Finland, France, The Netherlands, Portugal, Spain, and Turkey) covering the value chain for SecureGrid.

The SecureGrid is leaded by Otherthur (France).

The following drawing shows the overall consortium of partners per country, specifying the type of entity involved.



The consortium is made of 32 partners:

* 5 partners from Finland: 3 SMEs, 1 research centre and 1 University.
* 10 partners from France: 4 large industries, 1 SME, 2 research centres, 2 Universities
* 2 partners from Netherlands: 1 SME and 1 Research centre.
* 4 partners from Portugal: 2 SMEs, 1 research / academic partner and 1 end-user.
* 5 partners from Spain: 3 SMEs and 2 Universities.
* 6 Partners from Turkey: 1 large industry and 5 SMEs.

In total 5 large industries, 16 SMEs, 5 research centres, 5 Universities and 1 end user.

The expertise of the project partners cover the different activities to be developed in SecureGrid. The knowledge and skills contributed by the various project partners are complementary and cannot be found within a single European country. Trans-European cooperation is therefore a prerequisite for the successful undertaking of the SecureGrid project. This cooperation is expected to enhance synergies, to avoid overlapping efforts and possibly to enable joint market-oriented initiatives.

Each member of the consortium has been selected for their recognized expertise in one or more of project subject areas, in their compatibility of skills and their market position, especially applicable for the end-user.

There are many key industrial players having an essential role in the project, such as e.g. Oberthur, Gemalto, IRT SystemX, GDF Suez, Ericsson Turkey.

There are also 16 SMEs companies, mainly technology providers. Each of them will have a role in the business cases. SMEs will have the opportunity to exchange experiences with diverse research institutes, universities and industrial leaders of the Secure grid ecosystem.

In addition, the consortium has 10 high level research partners. The research partners of the project gain the possibility work with industrial companies around Europe, and that way get the opportunity to try out the research results on real industrial settings. The academics and technology providers will get very valuable industry feedback to develop better methods and tools and will gain references for future customer projects.

Finally there is one end user from Portugal, REFER that manages the infrastructure of the Portuguese Railway System.

The national and international cooperation will enable new business opportunities for all partners as well as possible new business offerings by combining different expertise and collaborating in building technologies and services.

* + 1. Cooperation added value: technology level

The SecureGrid project has 3 business cases (Water, Electricity and Gas). Each business case has its own targets, however, in technical level each of them need to create dynamic information business ecosystem in which the physical world is connected with business processes in real -time. There is no sense to make it separately for each business case, and therefore strong collaboration and added value is created by research and development of the SecureGrid technology framework together. The other strong motivation is the need for interoperability between business cases, for example, creation of smart business actions in energy market requires knowledge on the customer energy consumption and capability to control the power network grid.

The close collaboration between industry and research partners opens many possibilities for innovating new technologies for securing smart grids. With industry taking a strong role in the SecureGrid- project, these innovations have great potential to end up in new products and services. This in turn improves the security and reliability of the networks, which is a fundamental and necessary condition for many advanced smart environments such as smart cities and smart homes.

The consortium will provide novel research results for the consortium partners to further innovate technologies and services for securing smart grids. The industry partners will apply and improve their technology and service offering to match the needs of the grid. This will result in better security for the grid in the form of new technologies, new services and better understanding and management of the security related risks.

The following table shows that the partnership covers the whole value chain to successfully address the objectives of the SecureGrid project.

|  |  |  |  |
| --- | --- | --- | --- |
| Country | Partner | Type | Position in the value chain |
| Finland | Condenomicon | SME | Security/safety test automation |
| Finland | Indalgo Oy | SME | Provider of Mathematical Data Analysis Services |
| Finland | University of Oulu | UNI | Network security research |
| Finland | VTT | RES | Cyber security, network anomaly detection, cryptography |
| Finland | nSense | SME | Penetration testing, vulnerability assessments of web applications and networks, and PCI DSS services |
| France | CASSIDIAN | IND | Grid Security |
| France | CEA | RES | Grid Security |
| France | Citizen Data | SME | Machine Learning and Big Data platform |
| France | GDF Suez | IND | Gas & Electricity sales, generation and distribution |
| France | GEMALTO | IND | Security solutions and security services provider |
| France | Institut des Mines Telecom | RES | academic partner |
| France | IRT SystemX | RES | Multidisciplinary R&D in Complex Systems digital engineering |
| France | OBERTHUR | IND | Secure Element provider, Security Management |
| France | University of Burgundy | UNI | Communication networks, Communication Network Security, Intrusion Detction Systems, SmartGrid, Optimization |
| France | University of La Rochelle | UNI | University / Research |
| Netherlands | Target Holding | SME | Big Data Analytics, machine learning, artificial intelligence |
| Netherlands | IMEC | RES | Wireless technology for security in smart grids |
| Portugal | REFER | End user | Service development for maintenance and optimization |
| Portugal | EVOLEO | SME | Technology Provider |
| Portugal | IPBRICK | SME | Manufacturer and distributor in Corporate Solutions |
| Portugal | ISEP | RES | Smart Grids, AI techniques, Big Data |
| Spain | Answare | SME | Technology provider |
| Spain | Innovati | SME | Technological provider, solution provider and distributor |
| Spain | NIMBEO | SME | Technology Provider. Big Data, Smart Grid |
| Spain | Universidad Politécnica de Madrid | UNI | Technology provider, machine learning based on a Big Data Analytics platform |
| Spain | University of Madrid Carlos III | UNI | Artificial Intelligence, Semantic Technologies, Software-as-a-Service and Big Data in real-world scenarios |
| Turkey | BOR Yazilim | SME | Service development for maintenance and optimization |
| Turkey | DIA Yazilim | SME | Data Algorithms, Security, Service Development |
| Turkey | Ericsson | IND | Big Data Analytic For Smart Grids |
| Turkey | Hisbim Hisarlar | SME | Software developer, use case provider |
| Turkey | Phaymobile | SME | Service and Application Development, Security |
| Turkey | VAS Telekom | SME | Data Mining |

1. Work description
   1. Project structure

The project is structured around 7 Work Packages.

**WP1 Project Management**

It is the objective of this work package to establish the proper communications channels and set up the necessary controlling infrastructure in order to provide an adequate project management through the lifespan of this project. This includes the following detailed objectives:

* Monitor, track and supervise the progress on the project work packages.
* Control deviations that arise during the lifespan of the project due to changes in the scope, resources allocation, scheduling, etc.
* Manage the overall project according to approved plans
* Ensure that the required deliverables are prepared and presented on time and according to the established format.
* Guarantee that the required reporting is prepared and delivered properly.

**WP2 SecureGrid Scenarios (Water Management, Electricity, Gas)**

The goal of this work package is to investigate, develop and validate the technical and business requirements of the topics being proposed: communications components, central core (automated energy data management) and computational intelligence.

Subsequently requirements, scenarios, use cases, and core technologies that will guide the research work done in the remaining WP’s will be investigated.

This WP will also define the scope delimitation of the project itself.

**WP3 Grid Security**

The objective of this work package is to design and validate the security module components in smart grids.

This platform is based on the following principles:

* Strategic: a global level, the security in smart grids and the safe integration of these smart grids in all homes.
* Strong client side security thanks to the embedding inside devices of secure element remotely managed in a multitenant context.
* Technology: use of Artificial Intelligence tools and processing large amounts of data (BigData) to ensure the security in smart grids.

Another objective will be to ensure security and manage system in different environments:

* Ciber Security Management
* Physical Security Management
* Process and Domain Security
* Fraud detection.

**WP4 Deep Learning and Big Data Platform**

The objective of this package is to develop advanced analysis methods capable of making inferences about the large amount of data (Big Data) from the smart grid. Artificial Intelligence techniques detailed examination, including deep learning algorithms so that you can see which of them are best suited to the audited data. The challenge is to infer patterns in the security of smart grids in order to recommend corrective actions for the safe use of intelligent networks (smart grids).

**WP5 SecureGrid Architecture**

The goal of this work package is to develop and validate the system architecture and the functional framework specification.

This WP will be built on top of ongoing activities in WP1 and focus on the domain analysis of SecureGrid, in order to provide a system-wide model.

This model will take into account the existing standards and highlight the necessary evolution. Then, the final step will be focused on a high level implementation based on a Service Oriented Architecture of the system.

**WP6 Demos**

The aim of this package is to validate the system developed by the technologies and architecture mentioned in the previous packages.

The second goal of this work package is to set up demonstration applications using the developments of the project in order to:

o Illustrate and demonstrate the feasibility of the approach.

o Test different situations such as set-up, detection of special conditions, etc.

o Evaluate and assess the results of the project in a realistic environment.

Our system will be tested in different scenarios to control the management of resources (water, electricity, gas, others ...)

**WP7 Dissemination, Exploitation and Standards**

This workpackage is dedicated to the fundamental issues of dissemination, exploitation and standardisation promotion. In this way, its main objectives are:

* to spread the SmartGrid results in the industrial and scientific community,
* to disseminate knowledge to technical/scientific audience to raise the objectives targeted by SmartGrid.
* to propose project results in respective standardization activities

To this end we will ensure an overall consistent project-internal and public communication about the progress of the project.

The planning is as follows:



* 1. Main milestones

Exhaustive list of project milestones:

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Description | KPI | Completion month |
| MS1 | System requirements and scenarios defined | The requirements volatility calculated as number of requirements changed per week over the total number of requirements is lower than 0.05. All the scenarios should be defined | M6 |
| MS2 | Potential security attacks analyzed and security modules designed | 100% of the analysis of the list of security attacks, 95% of design of fraud detection module according to the requirements | M12 |
| MS3 | Deep Learning Algorithms and Big data platform analyzed and designed | 100% of the analysis and design of deep learning algorithms considering the type of information from all possible sources of data. 95% of the development and implementation of big data algorithms considering a high degree of data traffic | M18 |
| MS4 | Neural Networks for Prediction and Estimation and Big data platform implemented | 95% of the design and implementation of Neural Networks for Prediction and Estimation. Security Efficiency evaluated with a 99% success rate in detecting intrusions and less than 1 false alarm per hour. 100% of the implementation of Big Data Platform considering the possible sources of data according to the proposed scenarios | M24 |
| MS5 | Implementation of SecureGrid System v1 | System implementing 95% of the functionalities required. | M30 |
| MS6 | SecureGrid Platform implemented and evaluated in 3 different scenarios | SecureGrid Platform implementing 100% of the specifications integrated and running in the common framework and 95% of the development of evaluations designed | M36 |

1. Rationale for public funding (National Coordinators)

Auto-generated section: input to be provided only on the Community website. Do not edit or remove this box and do not provide any text within this annex in this chapter, but provide the requested information directly on the ITEA Community website.

On the website you must filling one section per country represented in the consortium. This section will indicate the national coordinator and detail the national rationale for funding. At the end of the national rationale for funding, the national coordinator has to indicate the national ICT clusters the project has contacted and intends to join (a clear status with regards to the cluster has to be indicated).

The national rationale for funding has four components:

* national gain: you have to explain the benefits for the participating countries (e.g. support to national strategies, standardisation, open source,knowledge dissemination, wellbeing improvement, impact on national productivity, etc.), how the country benefits from collaboration with other countries and the risk level of the investment (i.e. why is a public incentive preferred for such investments),
* return on investment (RoI): you have to explain how the money invested by both Public Authorities and companies is expected to generate value, revenue, jobs and/or economic growth, etc.,
* value creation of the national sub-consortium: how cross-fertilisation between the various participants is achieved;
* adequate balance between the national partners (e.g. ratio of effort as a percentage for academics, SMEs, etc.).

For each partner, in addition to contact details and a generic description (incl. type and size of the entity), two specific descriptions are requested:

* relevance of the partner within the project by describing its main role in the project and the main addedvalue to the international consortium and vice versa;
* market access, i.e. how the partner intends to exploit the project results and how the market(s) will be accessed(exploitation prospects and capability); current main markets and main customers, as well as planned exploitation plans and strategies are welcome whenever doable.

It is crucial that all national coordinators get in touch with their national Public Authorities (PAs) to present them the project (idea, partnership, budget, etc.), checking funding opportunities and ensuring that the national consortium is eligible, even in countries that are not part of the ITAC (ITEA Authorities Committee). Beware of eligibility issues at national level.

For ITAC countries, information on the contact persons is available on the ITEA public website (in section “Participate in ITEA / Funding”). For the EUREKA countries (see: <http://www.eurekanetwork.org>) that are not member of the ITAC, the contact persons are National Project Coordinators (NPCs); look for them on the following website page: <http://www.eurekanetwork.org/in-your-country>, using the “Select your country” button at the bottom of the page).

**Finland**

As a sparsely populated country, Finland needs the grids that form the critical infrastructure to be very robust both against accidental outages and malicious attacks. Thus, securing the smart grids is important for Finland in particular and globally in general. Furthermore, one aspect of the cybersecurity strategy of Finland is the security of critical infrastructure and this project clearly addresses one key element in this. The gains for the Finnish consortium are in developing new security methods for smart grids, which should lead to increased business opportunities both nationally and internationally. In addition, the improved security of these grids will benefit the nation as a whole.

**France**

Smart grids are a major challenge for energy production and consumption in a period when strategies must face Climate change and Economy recovery. For France today’s infrastructures situation will increase electricity price even if it is one the cheapest in Europe. Smart Grid are very important to include efficiency in energy management a multi-modal production (nuclear, wind, solar, hydroelectricity). It is important to foresee that the domain of smart grids implies a lot of questions. Indeed smart grids is the alliance of two domains energy and cybersecurity. Communications, that are bidirectional, require a greater security than the traditional networks. Energy, that is highy strategic by definition, has been targeted by many cyber-attacks like the most known one Stuxnet. Smart grids multiplying connection nodes can create a structural weakness. In addition smart grids generates more and more data, most of them are personal from the end-users point of view. Several demonstrators have been deployed in France under the supervision of ADEME. Security is not an option and the French consortium has clearly the right level of expertise and industrial potential to provide an adequate answer.

**The Netherlands**

The Netherlands has been a frontrunner in Energy Transition and has made significant investments in grid infrastructures for smart energy and smart city environments. There have also been various initiatives started in the Netherlands on Cyber Security, such as for instance ENCS, the European Network for Cyber Security. Current state-of-the-art methodologies are focused detecting and preventing intrusion, fraud, incidents and malfunctioning. This has led to collection of huge amounts of data from the critical grid infrastructures.

The next step is to discover and develop innovative analytics techniques that bring a secure grid to the next level. The application of Big Data analytics, machine learning and artificial intelligence techniques to the huge amounts of data gathered by the grid, is considered to crucial for reasoning on, knowledge over, planning (the prevention) of and learning from security breaches of critical grid infrastructures.

The Dutch consortium is driven by a complementary of 2 partners, (1) Target Holding, a SME focused on Big Data Analytics, machine learning and artificial intelligence on extreme large datasets, and (2) IMEC, a knowledge institute with extensive expertise on innovative hardware solutions for secure grids.

After the PO phase we will expand the current consortium to have all necessary expertise, know-how and business drivers for realizing the SecureGrids project. We have been in contact with large industries Thales and Alliander to pave the road to successful market introduction of the newly developed technologies on a world-wide scale.

**Portugal**

Huge investments in Distributed Generation and in smart metering for Smart Grids have been made all around the world and also in the EU and in Portugal. However, there is a lack of investment on platforms to ensure the required cybersecurity for smart grids resources connection with electrical networks and data transmitted by the smart meters and sensors. There is also a lack on methodologies to detect and prevent intrusion, fraud, incidents and mal functioning of the smart grid. The application of AI and Big Data analysis techniques to the huge amounts of data gathered by the Smart Grid is a step further that allows reasoning, gathering knowledge, planning intelligently and learning to efficiently manage security breaches. Protocols for the security transmission of data related to the smart grid, whether to control distributed resources or loads, or to assure privacy and security against intrusions and non-repudiation are crucial, moreover when related to a critical infrastructure, such as the electricity grid, that affects all sectors of a developed country: from health care, to industry, education, etc.

The Portuguese consortium is driven by a complementary and dynamic consortium of 4 partners having all the necessary expertise, know-how and business drivers for realizing the SecureGrids project. It is composed by two SMEs, Evoleo and IPBRICK, one research and academic partner, GECAD, and one end user, REFER.

Evoleo has a considerable expertise in monitoring and middleware, and addressing the smart grids market, by becoming an important player in this area, is part of the strategy of the company.

GECAD excellence area is the application of artificial intelligence, optimization, and decision-support techniques to engineering problems, with emphasis on power and energy system applications.

GECAD detains the knowledge about smart grids management methodologies, consumers profiling and distributed energy resources that is crucial to develop tools that detect, prevent and evaluate the impact of smart grids attacks, and how to act according to its level and type of impact. In this project secure communications are crucial, and this project approach will ensure the integration of mechanisms against cyber attacks, thus making it truly possible. IPBRICK will bring their competences on this area and reinforce their position in the power and electricity networks market, which is a goal for the short term.

Thus combining the skills of Evoleo, in sensors and middleware for smart grids, with the security in communications by IPBRICK and the AI applications being made by GECAD, the consortium is quite complete and able to develop a work covering all the value chain of SecureGrid project. Moreover, the immediate impact at the national level will be achieved by involving REFER, the Portuguese Railway Infrastructure Manager, as a pilot. REFER has a private electricity grid, with both Medium and Low Voltage distribution networks, to power locomotives and other rail subsystems. It is indeed a critical grid infrastructure, as REFER assures the railway service of Portugal. Grid security and fraud detection are major concerns of REFER.

All these aspects contribute positively to the recovery of the Portuguese economy, increasing the competitiveness of companies in different sectors and improving Portuguese citizens quality of life.

**Spain**

The Spanish consortium is composed by a well-balanced set of partners, having all the necessary expertise, know-how and business drivers for realizing the SecureGrids project. More in detail Spanish consortium has composed by three SME and two universities. With this distribution Spanish partners cover the most innovative research (universities) and the market real vision (SME).

Spanish set of partners has a complete expertise in different areas related with Secure Grid objectives. For example applying cutting-edge research based on Artificial Intelligence, Semantic Technologies, Software-as-a-Service and Big Data in real-world scenarios with potential impact in solving industry problems from an applied research standpoint and supported by a Big Data analytics platform. A Spanish partner has a commercial product based on these technologies (BIG DATA - Data Mining and Decision support system). This product will be the ideal platform to test different approaches and SecureGrids technologies.

The results of Secure Grids will make possible a quick market access and a robust way to ensure requests free of fraud.

Positive feedback received from the Public Authorities:

* Centre for Industrial Technological Development (CDTI): The Project is in line with the recent communication from the European Commission CE on security for smart grids in which electrical networks are considered as critical infrastructures

(<http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/20140409_enisa.pdf>),

Applying Big Data and AI techniques on a big volume of generated data could be an interesting application.

* Ministry of Industry, Energy and Tourism: Big Data is a priority at European level and therefore it is well received by our Administration.

**Turkey**

Distribution of electricity and management of natural resources are global top priorities and it is same in Turkey. Transformation from traditional infrastructures to the smart grid technologies arises some problems to solve as well as potential use cases to be implemented. By participating in the SecureGrid project, Turkish consortium would like to explore potential use cases such as dynamic management of electricity, gas and water networks on the grid architecture. Besides the potential scenarios, Turkish consortium will also work on developing solutions for the arising problems such as security issues. In order the reach the goals a well-balanced and strong Turkish consortium has been constructed. Consortium has partners from different expertise areas. Bor Software has strong experience in ITEA projects and will be the country coordinator. Bor will contribute to the project with analysis of data and algorithm development. Dia has a long time expertise on cloud systems. VAS Telekom is working on telecom platforms. Phaymobile, part of Cardtek Group, is an experienced partner in payment systems. Hisbim, part of Hisarlar Group, is an experienced partner in industrial environments and will be developing services and applications. Ericsson as an industrial partner will be the integrator and use case supplier besides the development activities on data analysis and M2M systems. We believe that results of the project has a high exploitation potential in Turkey and there is a strong and complementary Turkish consortium to achieve targeted results.

1. Summary of costs & effort breakdown

Auto-generated section: input to be provided only on the Community website. Do not edit or remove this box and do not provide any text within this annex in this chapter, but provide the requested information directly on the ITEA Community website.

This annex will contain a comprehensive summary of the costs and effort, by providing 1) costs & effort per country per WP (with totals), and 2) costs & effort per partner type. This data is automatically computed based on the detailed figures of costs& effort provided online by each partner on the Community website: it is therefore crucial that all partners provide relevant input for both costs & effort, and do not leave blank fields, which would generate erroneous breakdowns.

Detailed costs & effort per partner are provided in the related country perspective section of §4.