INNOVATION STRATEGY CLOSE-OUT REPORT

PROJECT TITLE	SUCCESS – Cyber Security in Future Networks An EU Funded H2020 Project
PROJECT OWNER	Karen McGeough, Strategy, Design & Business Process Manager, Networks Telecoms.
INTERNAL DOCUMENT NO	DOC-161019-FEW
VERSION	1.1
DATE	3rd March 2019

BRIEF OVERVIEW OF PROJECT & EXPECTED BENEFITS

Background

ESB Networks is continuously working to understand the risk of Cyber Security in the operation of a utility specific telecoms network. The production of electrical energy is becoming more decentralised and the grid is becoming an open system with a large number of players. Making the grid open requires the development of new technologies to ensure reliability of electricity supply.

This also requires operators of Critical Infrastructures to integrate their operational systems with Information and Communication Technologies (ICT). Due to the critical importance of the operations conducted by such Critical Infrastructures, security concepts must be developed and realised in all of them.

H2020 SUCCESS project

An opportunity was presented to ESB Networks in 2016 to become part of a consortium of European partners across industry to work together on an EU funded Horizon 2020 research project called SUCCESS. SUCCESS was centred around cyber security in critical infrastructures, such as electricity networks. The SUCCESS project addressed challenges in both the critical utility networks, and the communications networks and IT capabilities that support them.

This H2020 project aimed to design, develop and validate on small scale field trials, an adaptable security framework to significantly reduce the risks of cyber threats and attacks when smart metering devices are deployed across the grid in applications such as EV Charging systems, Solar PV, Demand Response and Battery Storage systems.

ESB Networks Role in the Project

Of the 16 partners, ESB Networks were one of three utilities taking part in the project, where the utility's role was to each provide a test environment for a specific use case. ESB Networks' selected use case was an EV charging system.

The Irish trial use case was a continuation from a previously completed EU H2020 project called Finesce. In project Finesce, a solution was developed to manage grid frequency through the controllability of a large number of widely distributed small loads, such as EV chargers. SUCCESS took this concept further by exploring the cyber related vulnerabilities with this grid management solution.

The Irish trial site (ESB Networks in Leopardstown) both hosted and integrated with a range of components, devices and software that were developed by other project partners in order to successfully emulate the detection of a mass attack on EV chargers.

The other utilities in the project were located in Romania and Italy, providing use cases on solar PV and small-scale storage and demand response. RWTH Aachen laboratory in Germany hosted many of the innovative software systems and related components that were developed in SUCCESS. These systems were remotely connected to each trial site for use case participation as well as use case assessment.

Figure 1: EV Charging Unit containing SUCCESS components, Leopardstown Road, Dublin

Key Objectives

The SUCCESS project contained a number of objectives to be realised as part of the research. A selection of key objectives related to the Irish trial are outlined below.

1. **Simulating the detection of a cyber attack**
   The first objective of the Irish trial was to simulate a number of cyber security threat vectors and determine the ability of the SUCCESS solution to detect such threats. For example, the detection of a cyber-attack involving a maliciously generated false EV load interrupt command from the DSO or TSO on a significant number of EV charging devices. Initially it may look like this instruction is coming from the grid operator to manage the frequency and ultimately the stability of the grid, but as it is maliciously generated through a cyber-attack, the operation could cause wide scale disruption and loss of service. The objective of the SUCCESS solution is to utilise the infrastructure developed by the project to capture accurate and verified measurements and send them to the grid operator over a secured and un-hackable communications channel.
2. **Low cost grid edge devices**
   Due to the projected large-scale deployment of metering applications across the distribution grid over the coming years, the cost of securing the network will be a challenge. A second key aim of the project was to develop low cost devices (such as Low-Cost PMUs) that provide the required functionality needed to maintain the highest level of security on the network.
3. **Pan-European Monitoring Solution**
   An interesting element of the project was the integration of the infrastructure at each of the three trial sites with a pan-European monitoring centre prototype located at a central location. It was expected that this system would provide the capability to detect cyber-attacks across multiple jurisdictions and multiple utilities, with the objective of informing other utilities and grid operators of potential imminent attacks.

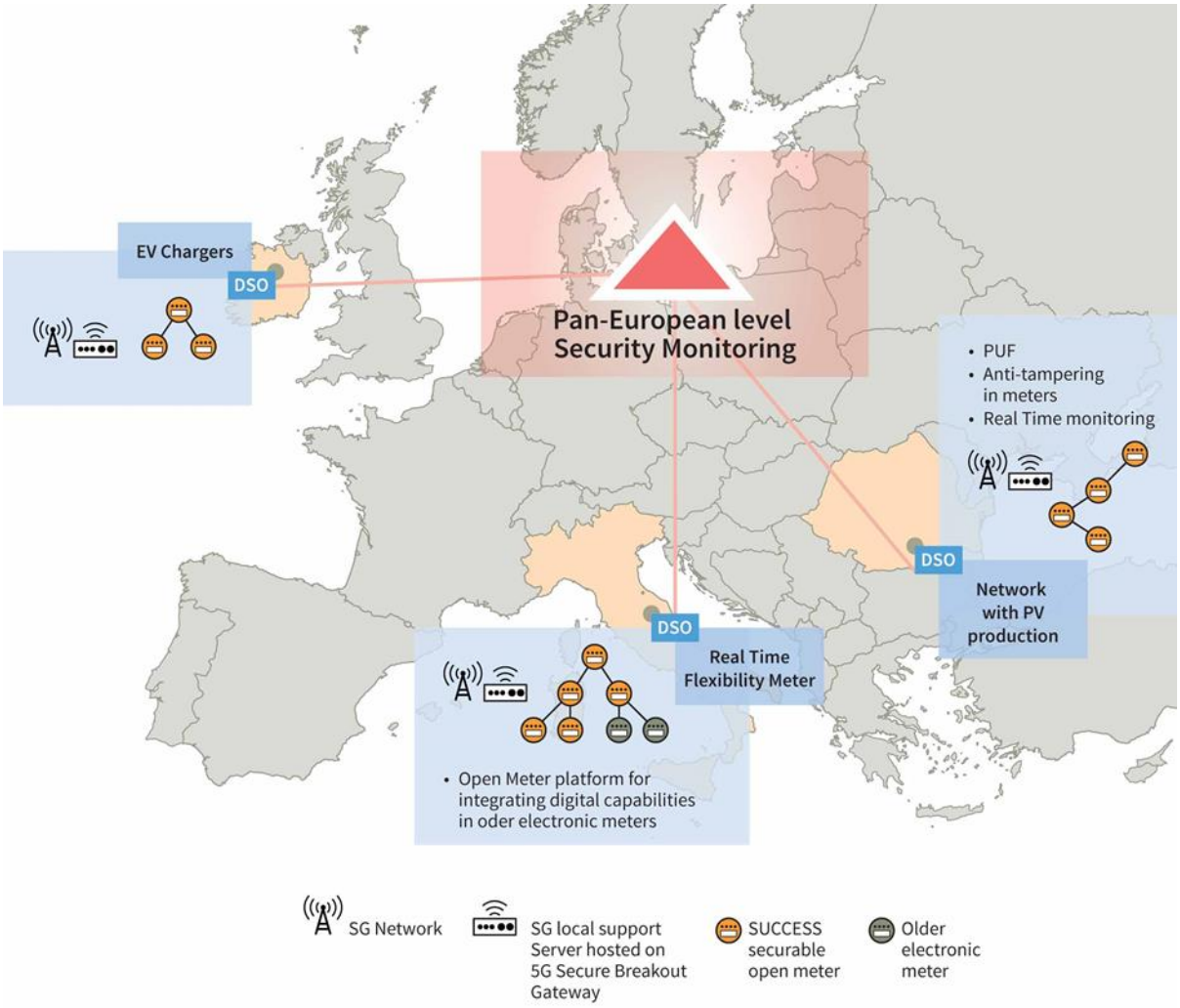

Figure 2: Three trial sites in SUCCESS project communicating with a Pan-European monitoring centre

Benefits to ESB Networks

It was expected that the learning from the collaboration on this project would provide opportunity to work with academics, engineering companies and also other utilities to get a well-rounded understanding of the challenges faced by different players in our industry, but more importantly to learn from the project partners ensuring the knowledge gained can be fed back into the design and operation of ESB Network's operational telecoms network that provides the visibility and controllability of the Irish electricity grid. This proved to be the case.

The project's website contains further information, including technical papers completed and published for each stage of the project.

www.success-energy.eu

RESULTS

The three trial sites were successfully delivered, following extensive collaboration with the project partners over the 30 months.

The various components developed by the project's engineering partners were deployed in the Irish trial site, and the trial site successfully communicated back to the monitoring centre solutions that were located in a lab environment in RWTH university in Germany. The monitoring centre solutions successfully simulated a response to an attack taking place on one grid only, and also simulated the response to an internationally coordinated attack, through the pan-European monitoring centre solution.

Scalability testing was successfully carried out to analyse the capability of the entire SUCCESS solution to be deployed across Europe.

The devices developed were low in cost, demonstrating that lower cost devices can still provide the required level of security, once configured to the correct and latest security standards. For a distribution system operator this reduces the potential challenge of cost when deployment of large numbers of secure grid edge devices is required.

Three successful open days took place in each of the trial site countries (Ireland, Romania and Italy) with a well-attended final event in Dublin for the end of the project, in conjunction with a final review meeting with EU appointed project reviewers.

All expenditure submitted was approved.

The project met all milestones and came in slightly under-budget.

Figure 3: Opening of the SUCCESS Final Event, Leopardstown Racecourse, Dublin, Nov 2018

Figure 4: Consortium Partners, SUCCESS Final Event, Dublin, November 2018

LEARNINGS

Significant learnings were realised through the collaboration with academics and engineering entities that were partners within the project.

The penetration of digitised control and metering devices deeper into the distribution grid is presenting challenges in terms of cost, capability and cyber security.

Learnings on the risks and vulnerabilities have created awareness across ESB Networks Telecoms on the areas that need to be focused on when designing telecoms solutions for connectivity of new Smart Grid applications, such as EV Charging infrastructure, PV / Solar systems, and small-scale storage solutions.

BENEFITS REALISED/VALIDATED

A Network of industry experts was created that can now be tapped into.

Knowledge on the vulnerabilities to be aware of with regard to cyber security has been developed.

Learnings have fed into initiatives such as penetrative testing / cyber security risk assessments that are now planned for ESB Networks telecoms networks.

NEXT STEPS – BAU, TRANSFER OF OWNERSHIP

The project closed in November 2018.

Post project completion, the infrastructure installed in the EV Charging system in Leopardstown was used by another H2020 project, RESERVE. However, planned decommissioning of all equipment from RESERVE and SUCCESS was completed in September 2019.

FINAL TIMELINES (REASONS FOR ANY DELAYS IF THEY OCCURRED)

No delays occurred.

FINAL COSTS

€304,972.89 was the final spend.