No 700416 SUCCESS

D7.1 v1.0

Progress Report

The research leading to these results has received funding from the European Union's Horizon 2020 Research and Innovation Programme, under Grant Agreement no 700416.

Contractual Date of Delivery	31.12.2017
Actual Date of Delivery	29.12.2017
Author	Fiona Williams, Ericsson
Participant	EDD
Workpackage	WP7 – SUCCESS Project Management
Security	PU
Nature:	Report
Version:	V1.0
Total number of pages:	18

Abstract:

This document provides an overview of the plans and progress of the SUCCESS project between its start on 1st May, 2016 and 31 October, 2017.

Keyword list:

Smart Devices, Threats, Security, Resilience, Survivability, Smart Infrastructure, Smart Metering, secure solutions

Executive Summary

The SUCCESS project is developing an overarching approach to threat analysis and the application of countermeasures with a special focus on the vulnerabilities introduced by Smart Meters. The project is designing and developing a novel holistic adaptable security framework which is being validated in small scale field trials. The framework will significantly reduce the risks of cyber threats and attacks when next generation real-time, scalable, unbundled smart meters are deployed in the smart power grid. These new meters will enable innovative applications and value added services within the emerging smart decentralized energy system paradigm.

SUCCESS will achieve this objective by encapsulating solutions to the key challenges of security, resilience, survivability and privacy in three use cases. The use cases will focus the Research, Implementation and Evaluation concepts of the projects on the needs of utilities.

In the first 18 months of its 30 months planned duration, the SUCCESS project has undertaken an extensive analysis of threats and countermeasures and has developed the first versions of the components of the SUCCESS Security Monitoring Solution for deployment in the three SUCCESS utility field trials, which will be completed in the second half of the project's duration. The planning of the field trials has been completed and the field trials are at an advanced stage of preparation. Additionally, the conceptual research work performed in the project in the areas of Security, Privacy, Resilience and Survivability has prepared the way for hardware-in-the-loop power network simulations of the concepts with 5G mobile communications, which will be performed in the second half of the project.

All goals for the period were achieved and all deliverables and milestones due were delivered. Exploitation plans for project results have been updated.

Authors

Partner	Name	e-mail
EDD		
	Fiona Williams	fiona.williams@ericsson.com
	Karina Nees-Maric	knm@k-aix.de

Table of Contents

1. Introduction

Living in a safe and secure society is a fundamental human need. Today's energy providers have really embraced change. Large-scale transformation is already happening in the energy sector due to the introduction of renewable energy, which is enabling consumers to become energy producers. At the same time, devices in the home, such as Smart Meters and Smart e-Vehicle chargers, can communicate directly with the utility, giving utilities more insight into the operation of their power networks. Electrical energy production is becoming decentralised and the grid is becoming an open system with a large number of players. Transforming the power grid into such an open system requires us to address now the challenge of developing new technologies to secure the reliability of the power grid as the opening of new digital interfaces introduces new vulnerabilities to the power grid.

The SUCCESS project will develop an overarching approach to threat and countermeasure analysis with a special focus on the vulnerabilities introduced by Smart Meters.

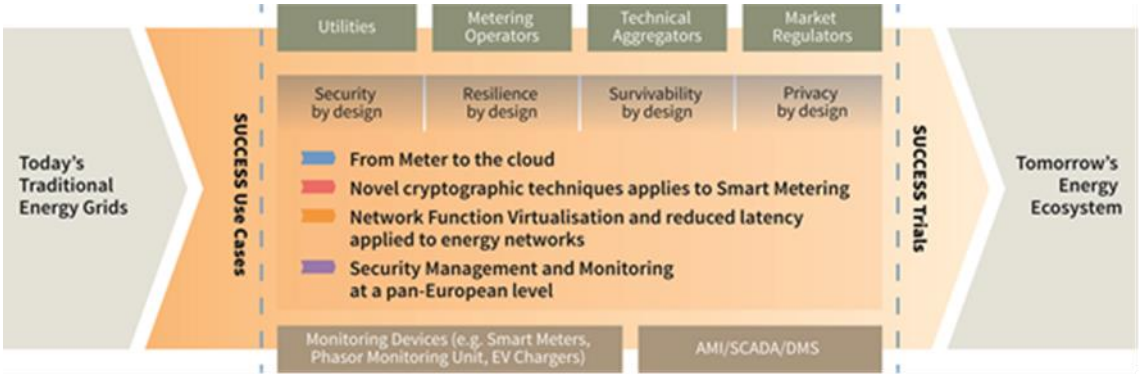

Figure 1 SUCCESS concept diagram

The project aims to design, develop, and validate in small-scale field trials, a novel holistic adaptable security framework. The framework will significantly reduce the risks of cyber threats and attacks when next-generation real-time, scalable, unbundled smart meters are deployed in the smart power grid. These new meters, when they are commercially available. will enable innovative applications and value added serviceswithin the emerging smart decentralized energy system paradigm.

SUCCESS will achieve this objective by encapsulating solutions to the key challenges of Security, Resilience, Survivability and Privacy in three use cases. The use cases will focus the esearch, Implementation and Evaluation concepts of the project on the needs of utilities.

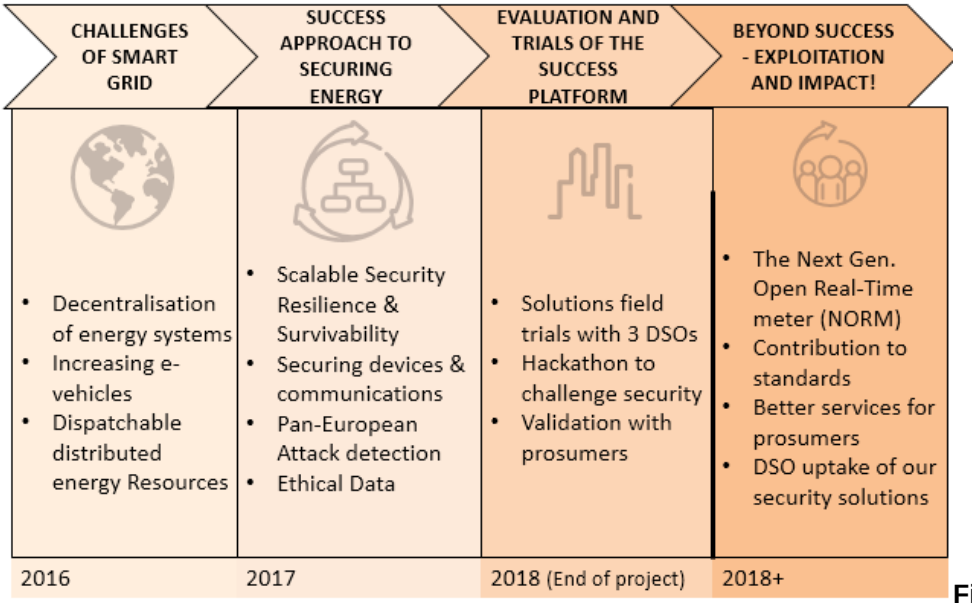

Figure 2 SUCCESS – from Challenges through to preparing commercialization

The SUCCESS concepts will drive investigations of threats and vulnerabilities of current and future Smart Meters, devices and networks, while the definition and implementation of countermeasures and their use in the SUCCESS field trials will demonstrate the countermeasures in a utility context. The SUCCESS project addresses both the power and communications networks of utilities and the IT capabilities that support them. It considers both of these infrastructures as they are currently used, as they will be used in 2020 with Next Generation functionality and finally as they will be used and designed in the years beyond 2030.

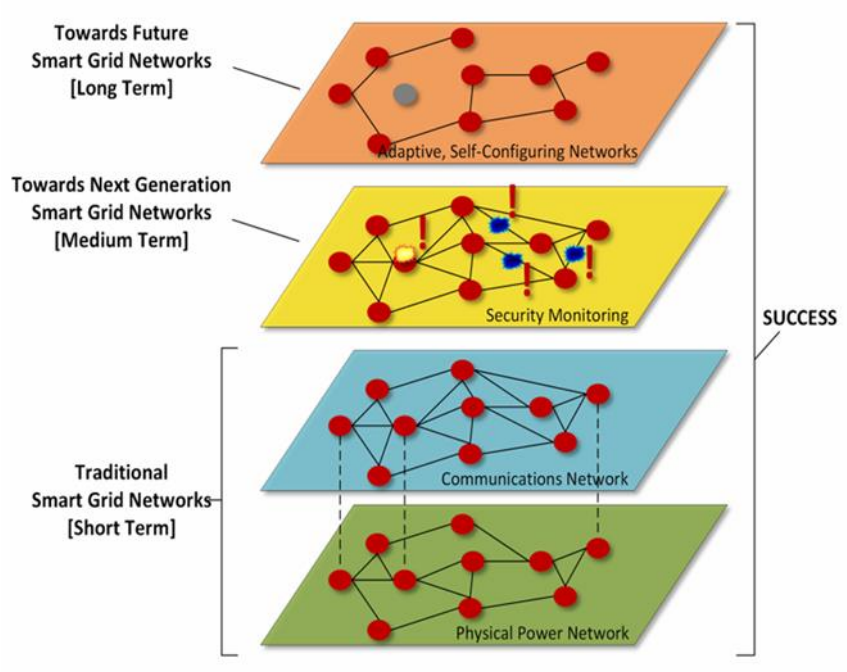

Figure 3 The SUCCESS scope

SUCCESS examines the interdependencies and exploits the potential interactions between the power grid infrastructure and the communications infrastructure used to control it, in order to use the interdependencies as countermeasures, embedding security, resilience and survivability in Future Smart Grid Networks. Security means both security of supply and resilience to all types of threats: not just Cyber-attacks but also adverse weather conditions such as storms or any other potentially disruptive events, such as loss of equipment.

1.1 Work undertaken by the SUCCESS project and main results achieved

In the period up to 31 October, 2017, the SUCCESS project has undertaken an extensive analysis of threats and countermeasures and has developed the first versions of the components of the SUCCESS Security Monitoring Solution for deployment in the SUCCESS utility field trials in the second half of the project. The planning of the field trials has been undertaken and the field trials' infrastructures are at an advanced stage of preparation. Additionally, the results of SUCCESS research concept development in the areas of security, privacy, resilience and survivability by design have prepared the way for power network simulations of the concepts with 5G mobile communications. Moreover, publications in well-known scientific journals and conferences have entrenched the acquired knowledge in the respective research.

All goals for the period were achieved. All deliverables and milestones due were delivered and future goals for the project are on track to be achieved by the end of the project.

1.2 Expected impact of project results

SUCCESS is developing a new approach to the security of the energy systems, guaranteeing their security of operation. The approach is based on new concepts for Security, Resilience and Survivability, as well as the implementation of Next Generation Open Real-time Smart Metering. The new concepts are being implemented as the SUCCESS Security Monitoring Solution, which supports a complete customer-centric automation architecture while preserving the privacy of the customers involved. Results of the SUCCESS project will provide short, medium, and long term improvements to securing power networks.

Starting from a security by design approach and placing resiliency and survivability in focus, a new joint design of both the Energy Infrastructure and the ICT Infrastructure is proposed. Building on the project's research results, our implementation approach is based on the definition of a Next-generation Open Real time smart Meter (NORM) as a key building block of our solution. NORM aims to secure the end nodes of the energy system while providing innovative services in a customer-centric grid. Secure local communications between customers and the distributed automation of grid operators will be provided in SUCCESS using fifth-generation mobile communications (5G) which provides edge cloud solutions including the option to execute functionality in processors co-located with the base station and sharing the same power supply. In SUCCESS, the edge cloud system will help ensure that the communications continue to operate during a grid failure, and will contribute to the rebuilding of the entire grid from the bottom giving a new option of Survivability by Design.

Additionally, because cyber-attacks are always possible, the SUCCESS architecture proposes the idea of Double Virtualisation to guarantee Resilience by Design. Double Virtualisation decouples data and functions in a virtual environment so that, in case of cyber-attack, it provides a countermeasure whereby the data or functionality can be moved to a different virtual computer and will continue to function, effectively thwarting the attack.

The scope of the domain addressed by SUCCESS is illustrated in Figure 4, which depicts the SUCCESS Security Monitoring Solution.

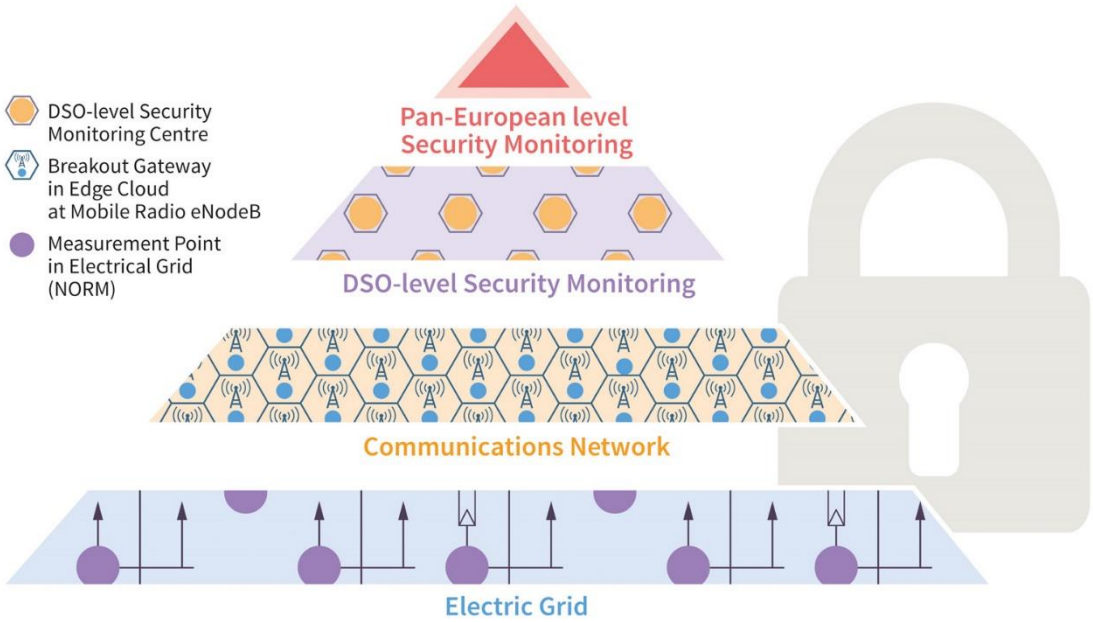

Figure 4 SUCCESS Security Monitoring Solution

The Security Monitoring functionality in SUCCESS applies a defence-in-depth approach, performing security threat detection analyses on the edge of the mobile communications networks, in the DSO's management system and on a Europe-wide basis. Monitoring information is collected and shared between these levels, as is information on security incidents. Countermeasures can be applied, both automatically at DSO-level and mobile-cell level, and subject to the operator's discretion.

The SUCCESS results, considered in their entirety, will ensure the security of Critical Energy infrastructures based on Smart Metering, by:

- Driving business innovations in customer-centric energy networks, through our up to date communications approach and our interactive services,
- Accelerating the growth of European service and product companies in the rapidly growing utility security markets with our research and innovation results, many of which are applicable to a wide range of IoT applications.
- Encouraging the creation of new jobs in growing companies through our innovation events and other communications activities and by involving respective audiences early in the development process,
- Promoting the uptake of SUCCESS results through workshops, publications, trade fairs, exhibitions and contributions to new courses targeting university students.

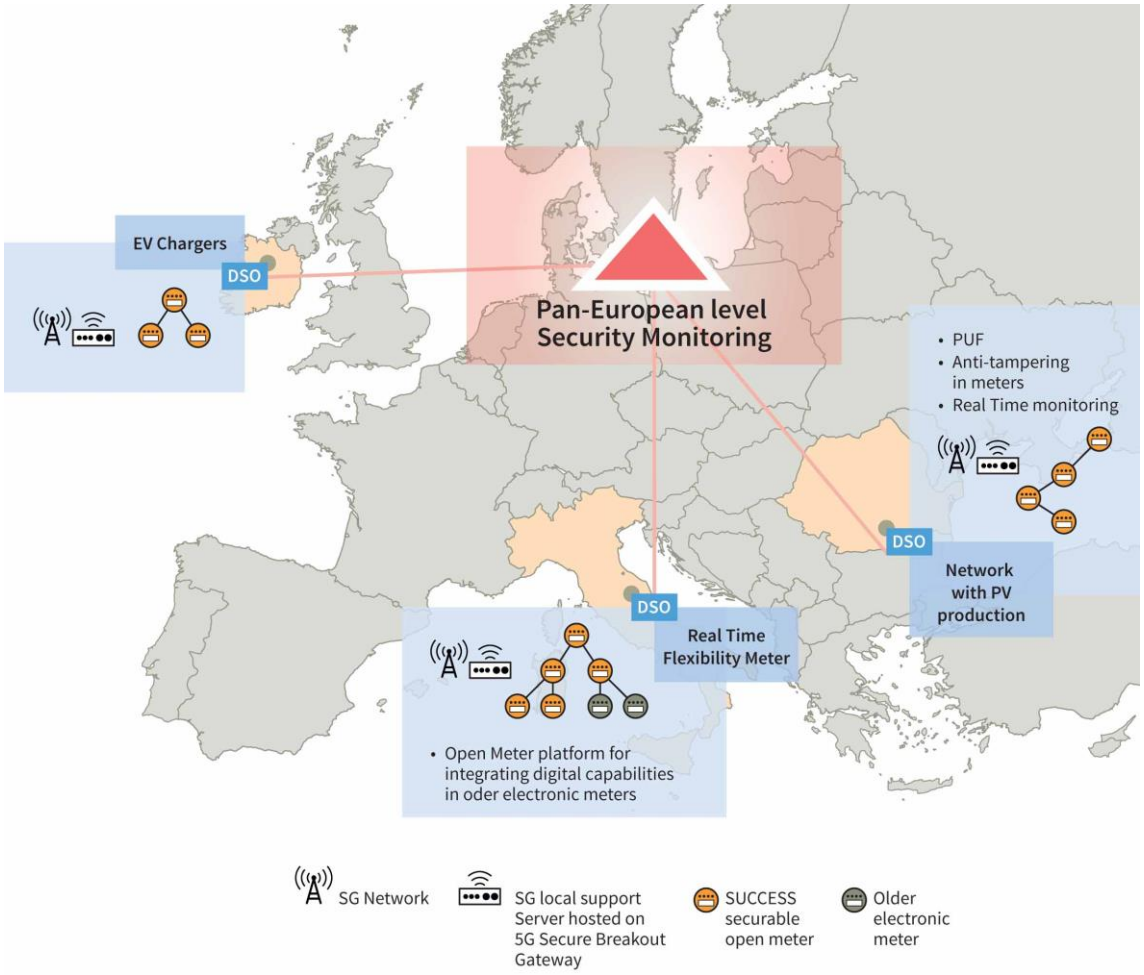

Figure 5 Trial site locations and technologies

The field trials will demonstrate results applicable to today's Smart Grid Networks (2017) and to Next Generation Smart Grid Networks (2020+). The trials, operated by DSOs in their infrastructures, will be located in Ireland, Italy and Romania. Simulations and modelling will be used to demonstrate results applicable to Future Smart Grid Networks (2030+).

2. Main achievements

2.1 Threats to smart devices

The primary objective of this work is to analyse the potential physical and cyber threats related to the Smart Grid "Access Network" (SGAN), which comprises the end-user devices in the lower layer of the Smart Grid hierarchy. These devices include the smart meters and new smart electronic devices (e.g. EV charging stations, Electric Storage Devices, PV systems) up to the DER Aggregators and in particular devices which are distributed in the grid and remotely operated.

Starting with the Smart Grid Architecture Model, the areas of interest to SUCCESS have been identified. A generic list of cybersecurity threats has been drawn up. This first list of threats was mainly related to the ICT industry in general and, after further analysis, a more specific listing tuned to the energy sector was produced. This list was further refined to make it more SUCCESS-centric so that the threats identified could be used for component and system testing during the three trials of the project. The methodology used for threat identification entailed the generic list of threats being categorised into various sections based on the ENISA taxonomy principles. A SUCCESS Security Monitoring Solution has been developed where all the appropriate threats identified could be tested with their corresponding countermeasures.

The main achievements on this topic are summarised here:

- The Smart Grid Architecture Model (SGAM) was extensively analysed. Areas of interest relevant to SUCCESS such as in the component and communication layers were identified . Based on this outcome, the relevant list of existing threats was determined and reported.
- Based on the identification of the existing threats targeting NaN (Neighbourhood Area Network) level devices and services, an extensive threat modelling has been performed. Techniques for identifying new, as yet unknown, threats have been developed.
- A classification of the identified threats based on the ENISA (European Union Agency for Network and Information Security) taxonomy principles has been performed, tailored to the scope, use cases and principles of SUCCESS, considering also the new attack entry points introduced by the SUCCESS components themselves.
- Relevant analysis employing comprehensive modelling based on attack trees and the STRIDE methodology has been undertaken. A literature review on threat classification and risk analysis and management has been performed. The relevant results were published in the project deliverable (D1.2) and presented at this year's ISGT conference in Turin.

2.2 Security resilience and survivability by design

The objectives of this work are to develop the new SUCCESS concepts of Security, Resilience and Survivability by design, by combining communications and IT technology to enhance the monitoring and automation of power distribution networks, thus increasing the security and quality of supply for both customers and operators.

As regards the **security by design** concept development, the main effort has been focused on securing Phasor Measurement Unit (PMU) time synchronisation. This decision is justified for two main reasons:

- firstly, the problem of time synchronisation security is notoriously difficult, and has not been fully understood in the context of PMUs; and
- secondly, PMU data is expected to be used for a variety of applications in future power systems, hence its security, including that of time synchronisation, is essential.

Traditionally the security of PMU time synchronization is ensured using IT solutions (e.g. cryptography) and the detection of anomalies is based on detection algorithms that consider IT

information only. On the other hand, data validity in power systems is usually verified using state estimation based on a physical model of the system.

The proposed security by design concept combines approaches developed in the power systems and in the IT sectors into a joint attack detection and mitigation scheme.

The work carried out during the first year of the project aimed at investigating the limits of power system based detection approaches, thus proving that a joint detection and mitigation approach is necessary, and on evaluating the effects of time-based attacks on the power grid and its reliability. The analysis focused on the study of possible time synchronization vulnerabilities, on both GPS time reference and PTP time synchronization algorithms, and their detection schemes. Numerical results have been reported on the effects of undetectable PMU time synchronization attacks on state estimation algorithms, resulting in a significant underestimation of the power flow on a transmission line. The outcome of such research activities has shown that reliance on state estimation only may be insufficient for detecting time synchronization attacks against PMUs. A methodology for identifying sets of PMUs that are vulnerable to undetectable time synchronization attacks has been provided.

The **resiliency by design** technique explored in the SUCCESS project is mainly based on the cloud-computing paradigm. In fact, grid automation architectures are increasingly migrating towards distributed cloud solutions, which offer unquestionable advantages in terms of scalability, together with being a natural candidate for the implementation of decentralised and hierarchical control and automation strategies. In this new scenario, system resilience can be enhanced by enabling fast relocation of cloud virtual resources when a security incident is identified. This mechanism is the base of the proposed Double Virtualization technique, developed in the first period of the SUCCESS project. The aim is to increase system resiliency (both from the IT and energy point of view) by exploiting cloud resources offered by the next generation breakout gateway (the so-called edge cloud).

In the first year of the project, the live migration algorithm for virtualized monitoring applications has been implemented and tested, together with the interaction with the other components of the SUCCESS Security Monitoring Solution, in particular those at DSO level (DSOSMC and DE-SMIS). A virtual Substation Automation Unit (SAU) has been deployed emantova@vub.ac.be in a cloud environment, together with a data streamer, emulating data flowing from the smart meters to the SAU. The implemented migration algorithm for Double Virtualization has been tested on this infrastructure, and has provided to be able to complete the migration of the state estimation functions from a virtual machine under attack to a new, safe, instance, without interrupting the execution of the monitoring functions.

The **survivability by design** concept is based on the exploitation of the distributed energy resources, nowadays widely available in the distribution grids, to implement a strategy to restore power after a blackout. The proposed methodology takes a bottom-up approach, energising small microgrids first and then reconnecting them together incrementally, which is the opposite of the currently employed grid restoration methodologies, which are top-down based, reflecting the traditional concept of a centralised power grid. With this assumption in mind, the proposed survivability by design concept considers the formation of microgrid clusters, where a microgrid that produces more energy than currently needed may supply electricity to another microgrid that faces the prospect of a blackout.

The main achievements on this topic are summarised here:

- For privacy by design, a set of recommendations on data privacy in smart grid security systems has been developed.
- For security by design, the limits of power-system-based attack detection approaches have been investigated, focusing on the effects of time-based attacks on the power grid and its reliability.
- For resilience by design, a migration algorithm for virtual applications on the cloud has been implemented and tested
- For survivability by design, a microgrid coordination algorithm for service restoration has been developed and tested in a lab environment.

More information is available in Deliverables D2.2, D2.4, D2.6, which are provided on the web page www.success-energy.eu.

2.3 Securing Smart Devices

The objective of this work is to secure smart devices through the development of an unbundled Next-generation Open Real time smart Meter (NORM) and a decision support system for DSO, named DSO Security Monitoring Centre (DSOSMC) , capable of detecting cyber-attacks on the distribution area of the grid and of applying a proper set of countermeasures from a set of designed reactive responses.

The energy sector has to face the continued increasing complexity of smart grids as cyber-physical systems. The expansion of intelligent networked devices throughout the energy distribution system, together with the supporting integrated communications networks, creates an urgent requirement for a coordinated energy cyber-security strategy. For this reason, it is an urgent necessity for market actors and utilities to provide themselves with solutions tailored for defending themselves against cyber threats.

The main achievements on this topic are summarised here:

- The design and initial development of a countermeasure dashboard toolbox named by SUCCESS as the DSOSMC (DSO Security Monitoring Centre) which determines the most appropriate set of countermeasures to be applied to the detected incidents and related threats impacting to the NaN level of the smart grid. The design of the hardware security module of SUCCESS and related first drop of basic functionalities was completed. An initial prototypee version of the unbundled NORM smart meter, was developed.
- The identification of component features, ensuring that the certification approach is properly defined, was undertaken.
- The identification and establishment of the certification guidelines was completed.
- The definition of a comprehensive set of Electromagnetic Interference tests to assess the resilience of the PUF feature embedded in the NORM platform when operating in a real environment in a power grid was undertaken and completed.

More information is available in Deliverables D3.4. D3.5, D3.7, D3.10, D3.11, D3.13 which are provided on the web page www.success-energy.eu.

2.4 Securing Smart Infrastructure

The main objective of this work is to define the SUCCESS reference architecture for Smart Metering and Power Network ICT security infrastructure, for the project trials and use case validation. Some of the new components identified as part of the SUCCESS architecture are defined in more detail and are being realized, allowing subsequent test-bed integration.

Besides the definition of the different architectures of the field trials and the resulting solutions, a systematic identification of countermeasures is being provided, which will help to determine solution impacts. A key component that has a central role for real-time orchestration and recommendation of countermeasures based on big data processing is the pan-European monitoring centre, which provides the means to analyse data from underlying DSOs in order to detect cyber-security incidents and to make countermeasures available to the DSOs.

In the early stages of the work on this issue, initially identified threats were analysed to determine the demands and implications on the high-level architecture and solution design. After the initial concepts for the SUCCESS architecture and solution were sketched and the threat analysis delivered, more detailed demands for countermeasures, and the analysis of the countermeasures were undertaken in a second iteration of the study. Impacts on software functions and infrastructure were determined and documented per countermeasure. In parallel, the demands on test and integration were identified and a test and an integration strategy was subsequently planned.

The main achievements on this topic are summarised here:

- Based on the outcome of the “threat identification and analysis”, a comprehensive list of countermeasures was identified and described.
- All the countermeasures were taken into consideration for the development of different components of the SUCCESS architecture.
- A corresponding solution description was created and structured so that it covers domains for utility, security and communication.
- To realise the solution several hardware/software components have been implemented in WP4, including the following:
    - The Breakout Gateway: a new network function to realise local edge processing and real-time countermeasure implementation,
    - A function for data integrity protection has been defined and implemented based on Data Centric Security, it allows detection of attacks related to data manipulation, for example of metering data,
    - A solution has been defined allowing edge authentication based on Generic Bootstrapping Architecture (GBA). GBA is a 3GPP standard which leverages the SIM security from mobile networks, enabling authentication of applications running on top,
    - The Pan-European Monitoring Centre: A monitoring function realised at DSO/TSO and pan-European level. The solution component at DSO level is named DE-SMIS and at the pan-European level is called E-SMIS.
- A plan was created on how to integrate these above components and to test the functionality which will be later utilised in to WP5 for the field trials.
- An overview of a component taxonomy to be used in the certification process has been created.

More information is available in Deliverables D4.1, D4.2, D4.4, D4.4V2, D4.5, D4.7, D4.8, which are provided on the web page www.success-energy.eu.

2.5 Demonstration of Secure Solutions for Smart Metering

The objective of this work is to evaluate and enhance SUCCESS designs, to plan and implement a set of use cases in three trial sites, addressing large-scale implementation issues, grid integration, communications network impact and security systems integration. The use cases will involve cyber-attacks being emulated, so that the detection of the attacks and the execution of mitigating countermeasures by the SUCCESS Security Monitoring Solution can be verified. Another objective is to undertake system penetration testing and scalability analysis to reinforce the design.

Since the commencement of the project, work has been carried out to develop the details of the architecture and components for the three trial sites. Included in this architecture are the interconnections and data flows between the individual components of the trial sites.

Effort was spent understanding the structure of the NORM device and how it will integrate into the trial sites, and also to understand the various technical requirements of the NORM such as physical connections, including electrical and communication interfaces, synchronisation requirements, physical housing and safety requirements for the device.

Use cases which emulate appropriate threats at each of the trial sites were selected and co-ordinated between the project partners. Following the selection of the specific threats, mapping of the relevant countermeasures to the overall SUCCESS framework was carried out.

The main achievements on this topic are summarised here:

- Validation of the trial objectives, functions, architecture and components for the three trial sites with other relevant work packages.
- Development of use cases for each of the trials, documented in Deliverable D5.1.
- Confirmation on how the NORM will be connected and integrated into the trial sites.
- Coordination of appropriate threats and countermeasures for each of the trial sites.
- Laboratory deployment in the RWTH lab with interconnections to P3E premises for interconnection with D-SMIS.
- Developing test plans for components and component integration.
- Completed analysis of trial data, confirming that the trials will not generate personal data.

More information is available in Deliverables D5.1, D5.2 and D5.7 which are provided on the web page www.success-energy.eu.

2.6 Generating Impact with SUCCESS

The work on this issue aims to maximize the scientific, industrial and societal impact of the SUCCESS project, with the main objective of creating awareness of the technologies and innovation activities within the project. In addition, our goal is to receive guiding feedback from relevant sector actors through their involvement in our events and communications and to trigger applied innovation based on the results of SUCCESS.

At the beginning of SUCCESS, the priority was to create a project design concept,which would convey the main concepts of SUCCESS (security and energy) through visual association. The project design includes color palettes, a cogent logo and the first dissemination tools that enable the project to address the community in a professional, consistent, qualitative and appealing way.

Most significantly, the project webpage went online practically immediately after concluding the project design. Social channels such as the Twitter™, Youtube™ as well as a LinkedIn™ account of the SUCCESS project were established and are regularly updated to provide immediate feedback from the interested community regarding further updates and possible cooperation.

Furthermore, significant steps have been made towards establishing a podium in relevant standardization organizations. SUCCESS activities are being promoted at the standardization bodies and the relevant events, and project partners were invited to give to presentations of the progress of our activities and outcomes during forthcoming meetings in respective groups. Project partners have been attending and examining contributions in the following standardization organizations: ETSI TC-Cyber; ETSI TC-M2M, oneM2M; ETSI MEC; IEC MEC; 3GPP SA6; IEC CEN-CENELEC; EOS; EU Smart Grid Coordination Group; CIGRE WG B5, B3, D2; IEFT CORE; IEFT Privacy and Security Program; WELMEC. Already in Year 1, SUCCESS was presented at the IEC CEN-CENELEC and the ETSI TC-Cyber group. In the latter, a work item suggestion with SUCCESS content is being prepared which will be filed in the oncoming meeting. Furthermore, a contribution is planned for the CIGRE working group in the fall of 2017. Standardization is one of the main channels for medium and long-term impact for SUCCESS which will continue to address the relevant bodies, by informing them about the scientific findings concerning the security and cyber-vulnerability of Smart Metering and Grid Control Infrastructures and by formulating eventual needed updates of standards. In addition, the advisory board has been set up and a first meeting of the Board was held on 9th of June, 2017 in Stockholm.

Well targeted and placed events were organised in order to entrench SUCCESS in the research landscape by pursuing personal contacts, achieving the personalisation of SUCCESS contributions through the partners and conveying a message of “immediate feedback” into the innovation loop of the project. The strategic goal of the SUCCESS events is to trigger open discussions, to facilitate collaborations and to spark innovation in the overlapping domains of energy, security and ICT. The concept was adjusted according to a multi-faceted target audience.

The main achievements on this topic are summarised here:

- SUCCESS has created a wide range of dissemination tools and active channels through which we constantly share knowledge and related content, receive feedback and promote dialogue.
- SUCCESS has organised and participated in a number of targeted events and has planned even more in order to share stimulating knowledge and ideas with explicit calls over social media for SMEs.
- SUCCESS has been particularly active in standardization bodies in order to entrench new knowledge in the medium term high impact channels.
- SUCCESS has analysed the certification approach of a range of different sectors (ICT, IT, Energy) and of different European countries and has derived proposals for a certification approach for the individual SUCCESS components as well as for integrated SUCCESS solution parts.

More information is available in Deliverables D6.1, D6.2, D6.4, D6.5, D6.7, D6.9, D6.10, which are provided on the web page www.success-energy.eu.

3. Conclusions

The SUCCESS project has achieved its interim objectives in the first 18 months of operation and is on target to achieve the project goals as planned during the second half of the project. The operation of the field trials and the generation of impact with the project results are in focus in the second half of the project.

4. List of Abbreviations

B2B	Business to Business
BMS	Building management system
CAPEX	CAPital EXpenditure
CENELEC	European Committee for Electro technical Standardization
CEP	Complex Event Processing
COTS	Commercial off-the-shelf
CPMS	Charge Point Management System
CSA	Cloud Security Alliance
EMS	Decentralised energy management system
DER	Distributed Energy Resources
DMS	Distribution Management System
DMTF	Distributed Management Taskforce
DSE	Domain Specific Enabler
EAC	Exploitation Activities Coordinator
ERP	Enterprise Resource Planning
ESB	Electricity Supply Board
ESCO	Energy Service Companies
ESO	European Standardisation Organisations
ETP	European Technology Platform
ETSI	European Telecommunications Standards Institute
GE	Generic Enabler
HEMS	Home Energy Management System
HV	High Voltage
I2ND	Interfaces to the Network and Devices
ICT	Information and Communication Technology
IEC	International Electro-technical Commission
IoT	Internet of Things
KPI	Key Performance Indicator
LV	Low Voltage
M2M	Machine to Machine
MPLS	Multiprotocol Label Switching

MV	Medium Voltage
NaN	Neighbourhood Area Network
NIST	National Institute of Standards and Technology
O&M	Operations and maintenance
OPEX	OPerational EXpenditure
PM	Project Manager
PMT	Project Management Team
PPP	Public Private Partnership
QEG	Quality Evaluation Group
S3C	Service Capacity; Capability; Connectivity
SCADA	Supervisory Control and Data Acquisition
SDH	Synchronous Digital Hierarchy
SDN	Software defined Networks
SDOs	Standards Development Organisations
SET	Strategic Energy Technology
SET	Strategic Energy Technology
SG-CG	Smart Grid Coordination Group
SGSG	Smart Grid Stakeholders Group
SME	Small & Medium Enterprise
SoA	State of the Art
SON	Self Organizing Network
SS	Secondary Substation
TL	Task Leader
TM	Technical Manager
VPP	Virtual Power Plant
WP	Work Package
WPL	Work Package Leader