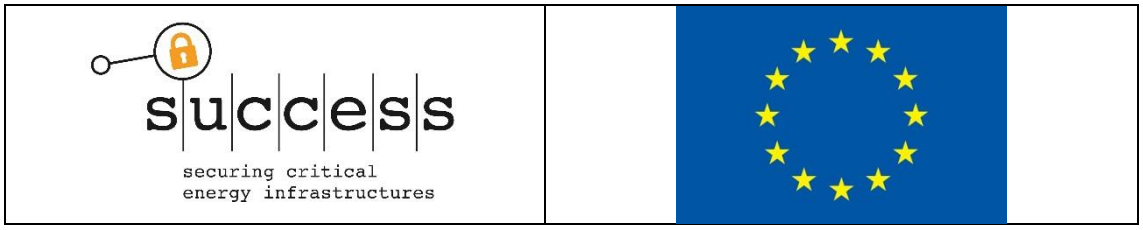

SUCCESS

D4.7v1.0

Integration and Validation Plan. Test and certification specifications

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.

Project Name	SUCCESS
Contractual Delivery Date:	31.01.2017
Actual Delivery Date:	**12.04.2017**
Contributors:	ENG, EDD, P3E
Workpackage:	WP4 – Securing Smart Infrastructure
Security:	**PU** = Public
Nature:	**R** = Report
Version:	2.3
Total number of pages:	19

Abstract:
This deliverable presents the initial results from Task 4.5 "Integration, Testing and certification" of the SUCCESS Security Monitoring Solution and covers both component testing of the individual components produced by WP4 and the integration among all the components of success solution. Moreover, this deliverable outlines the necessary processes and the associated methodology for certification of the SUCCESS Security Monitoring Solution.

Keyword list:

Security, communication, Utility, Architecture, Threat, Countermeasure, Integration, Validation, Testing, certification

Executive Summary

Individual component testing and system integration of these components have the goal of proving that the features developed for a software and hardware architecture work together well. Generally, the larger and more complex the project is, the more important is the integration testing.

In the case of the SUCCESS Security Monitoring Solution, the testing of the individual components of the SUCCESS Security Monitoring Solution and the system integration of these components has the additional goal of producing an integrated system which can be used by the SUCCESS field trial sites.

Component testing is performed on all components individually. Integration testing is performed after component testing, integrating the components which have been tested separately to produce a fully tested system.

In SUCCESS, it is not planned to perform the system integration at a single location. Also, the components are produced by several partners in different location and the component testing will be performed by the respective partners producing each component.

The method that will be used to perform the system integration is, first, to perform a set of pairwise integrations of component pairs which have common interfaces. In a second step these component pairs will then be integrated, resulting in a full system integration, with the individual components of the integrated system being physically located in different locations. This integration will be tailored on the trial sites' needs that are well described in the Use Cases.

This first version of this deliverable documents the preliminary plan for single component testing in WP4 and paves the way towards the preliminary plan for integration of the entire solution. In the first plan for the integration of the SUCCESS Security Monitoring Solution we describe also the approach that will be adopted in SUCCESS for certification. There will be two more versions of this deliverable later in the project which will provide more detailed planning of the individual component testing and the system integration tests.

Document History

Date	Revision	Comment	Author/Editor	Affiliation
20-11-2016	V0.1	ToC	Antonello Corsi	ENG
10-12-2016	V0.2	Added introduction	Antonello Corsi	ENG
15-12-2016	V0.3	Re-shape of ToC	Antonello Corsi	ENG
20-12-2016	V0.4	Add certification content	Paschalidis, Panagiotis	P3C
10-01-2017	V0.5	Add textabout testing	Zain Medhi	EDD
20-01-2017	V0.7	Finalize	Giampaolo Fiorentino	ENG
01-02-2017	V0.8	Added Contribute	Manuel Allohff	P3E
18-02-2017	V2.0	Available for review	Giampaolo Fiorentino	ENG
23-02-2017	V2.1	Internal review	Ganesh Sauba	DNVGL
03-03-2017	V2.2	Internal review	György Dán	KTH
12-04-2017	V2.3	Final version	Fiona Williams	EDD

Authors

Partner	Name	e-mail
P3C		
	Paschalidis, Panagiotis	Panagiotis.Paschalidis@p3-group.com
ENGINEERING (ENG)		
	Antonello Corsi Giampaolo Fiorentino	antonello.corsi@eng.it giampaolo.fiorentino@eng.it
ERICSSON (EDD)		
	Zain Mehdi	zain.mehdi@ericcsson.com
P3E		
	Manuel Allhoff	Manuel.Allhoff@p3-group.com
Romanian Energy Center		
	Mihai Sanduleac Mihai Paun	mihai.sanduleac@crenerg.org mihai.paun@crenerg.org

Table of Contents

1. Introduction

This first version of deliverable D4.7 presents initial results from Task *T4.5 – Integration Testing and certification*, providing both the individual test plan for individual components produced in WP4 (E-SMIS, DE-SMIS and Break-Out Gateway (BR-GW).) and the integration of these components with the ones that are produced by WP3 (NORM and DSOSMC (DSO Security Monitoring Centre) together with the double virtualization solution expressed in WP2.

Deliverable D4.7 is the first of three deliverables [1][2][3] for integrating, certifying and testing components in the whole SUCCESS Security Monitoring Solution.

This first version describes the initial version of the testing procedures planned for WP4 components, and the strategy for performing a pairwise integration of the components and solutions produced by WP3, WP2 and WP4.

Finally, a plan for the integration of the whole success solution will be provided. For this reason, a draft version of the testing time-plan, including deadlines for testing and integration with related drop of results will also be provided.

The document is structured as follows:

Section 2 gives a brief introduction to the SUCCESS infrastructure in terms of components. Chapter 3 introduces the single component test plan for WP4 components (E-SMIS, DE-SMIS and Break-out Gateway) and the plan for performing integration among WP3, WP4 and WP2 components. Chapter 4 describes the certification plan that will be used for address certification of the SUCCESS Security Solution.

2. SUCCESS Security Monitoring Solution

The entire *success security monitoring solution* is deeply described in the deliverable D4.4[4]. Figure 1 is taken from D4.4 with the intention to ease the explanation of the whole success solution architecture. The figure depicts the *success security monitoring solution architecture*, which is based on five main components and related interfaces that compose the entire architecture of SUCCESS. It is useful to recall some brief descriptions of the architecture, taking in account that a more in-depth description is presented in D4.4 [4].

The Figure 1 shows that the Security Monitoring components are located in two main layers: the DSO/TSO level, and the Pan-European level. E-SMIS and DE-SMIS are part of Pan-European Security Monitoring Centre (ESMC). They are made up of a single European-level Security Monitoring and Information System (E-SMIS) and several decentralised E-SMIS instances (called DE-SMIS). DE-SMIS collects data coming form edge-cloud resource and the DSO Security Monitoring Centre (DSOSMC). DSOSMC, thorougly described in D3.4 [1], collects data coming from New-generation Open Real time smart Meter (NORM) devices both through Break-out Gateway and directly.

Proceeding with a bottom up approach from real data measurements to DSO/TSO level, as shown in Figure 1**Error! Reference source not found.**, the first component that we meet is the NORM device. It is located in the distribution grid and measures prosumer and grid data.

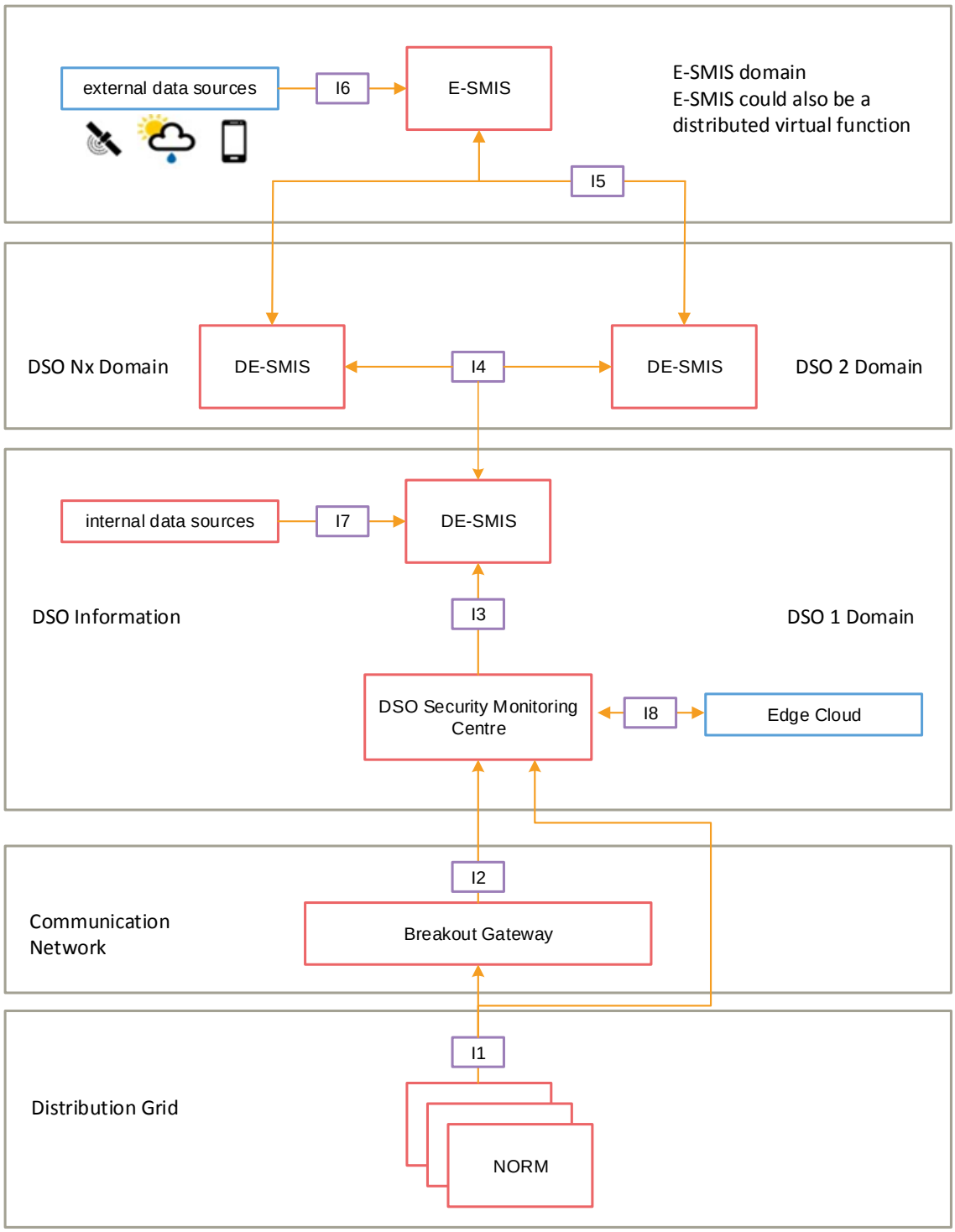

Figure 1 - success solution

As described in D3.4 [1], NORM provides to a DSO Security Monitoring Centre (DSOSMC) a set of basic measurements: voltages, frequency and phase measurements data, together with a minimal processing that may reveal potential anomalies in the data. The communication happens both directly over Interface 1(*I1*) and through an internal Security Agent or over Interface 2 (*I2*), via BR-GW which is a component in the 5G mobile network that allows mobile core network functionalities to be implemented close to the access and introduces new security-related functions [2].

Summurizing, the DSOSMC analyses the data caught on NORMs and the data comes from edge cloud over Interface 8 (*I8*). DSOSMC analyses them, detects anomalies in the received data to suggest a set of countermeasures to tackle the identified threat. After this analysis data are sent

to DE-SMIS instance - over Interface 3 (*I3*) - at DSO/TSO level. At this DSO/TSO level, DE-SMIS applies data mining methods on the data coming from DSOSMC, the internal data resource - Interface I7 (*I7*) and other DE-SMIS instances located at other DSO/TSOs (see Interface I4)- to provide local information to E-SMIS. E-SMIS gathers all data from DE-SMIS instances – over Interface 5 (*I5*)- to analyse and detect possible threats at pan-European level. At this level, it is possible to detect threats that are impossible to detect at local level.

The deliverables D3.10 [3], D4.4. [4] report a more details about the single components functionalities of the *success security monitoring solution* architecture.

3. Test and Integration Plan

This deliverable aims at providing an early individual test plan for the components produced in WP4: Break Out Gateway, and ESMC solution composed by DE-SMIS and E-SMIS and then an integration plan of the whole success security monitoring solution.

In the D3.10 the individual tests performed for NORM and for DSOSMC as two single independent components are described, they are part of WP3. In the same deliverable their integration test (I3 depicted in Figure 1) is also described.

This deliverable plans *the* **individual Components tests** for all **WP4** *success monitoring security solution components*. Initially, individual tests will be performed on each single component: BR-GW, DE-SMIS, E-SMIS. After that, integration tests are performed as follows:

- **Pairwise integration** of the components of the *success security monitoring solution*:
  - [NORM – BR-GW], [NORM – DSOSMC] *(I1)*,
  - [DSOSMC – Edge Cloud] *(I8)*
  - [BR-GW – DSOSMC] *(I2)*,
  - ESMC:
    - [DE-SMIS – DE-SMIS] (*I4)*
    - [E-SMIS – DE-SMIS] *(I5)*
    - [E-SMIS – external data source] *(I6)*
    - [DE-SMIS – internal data source] *(I7)*

- **Integration of success security monitoring solution** connects two parts of the whole solution: the NAN level with pan-European level [ESMC – DSOSMC] *(I3)* building up the *success security monitoring solution*.

Pairwise integration means that after the components have been tested individually as stand-alone components, the components will be tested in pairs. For each pair, the result of the testing will be to assure that the two components work correctly together and with their common communication interface tested.

This approach allows full system integration to be performed without needing to have one partner nominated to host the system integration activities on their premises. Each partner producing a component will host that component during the system integration, and the system integration (pairwise and further integration of pairs) will be performed using the components located at several locations.

This means that the SUCCESS field trials will build their trial sites based on the individual components produced (i.e. they will not receive a single, integrated system). However, these components will have gone through system integration testing as outlined above.

Therefore, the integration will be further described in the real implementation of trial sites that will be described in WP5 and reported in [5]. The test release refers to the end of the month (MXX stands for the last day of MXX)

As aforementioned, the plan for pairwise integration is the following:

- [NORM – BR-GW] , [NORM – DSOSMC] *(I1)*,
- [DSOSMC – Edge Cloud] *(I8)*
- [BR-GW – DSOSMC] *(I2)*

- ESMC
  - [DE-SMIS – DE-SMIS] *(I4)*
  - [DE-SMIS – E-SMIS] *(I5)*,
  - [DE-SMIS – internal resource] , *(I7)*
  - [E-SMIS – external resource] *(I6)*,

In this chapter and successive subchapters we provide an introduction to each individual single component with a functional description and a preliminary test plan. Then, the pairwise integration will be descripted, including the data flow between components as well as the deadline for both the drop of the integration and single test results. Finally, the integration of the whole solution will be described.

3.1 Test plan for individual WP4 components

The goal of this chapter is to provide a preliminary strategy and plan that will be followed in the realization of the single component testing that belongs to WP4, namely:

- Break-Out Gateway
- DE-SMIS
- E-SMIS

The following subchapters introduce the plan and approaches in a preliminary manner. The next versions of this deliverable will complete the sections that are not possible to describe at this stage of the project as well as to describe the testing plan deeply. In this document, we will provide data about drops of incrementally test integration for every component.

3.1.1 Break Out Gateway Test

3.1.1.1 Functional description

The BR-GW allows the implementation of real time countermeasures through breakout strategies using edge processing mechanisms for real-time applications that are being developed for the SUCCESS architecture. As such breakout gateway can enable distributed data processing, which is necessary for the realization of real time countermeasures at the network edge. Corresponding functions based upon this component will help reduce the impact of local failures and minimize response times.

In the next version of the deliverable a list of the detailed functionalities will be provided that will be implemented and tested for this component.

3.1.1.2 Test Strategy

The implementation of the BR-GW is handled in the context of *T4.4 - Enhanced communication solution development*. The following steps describe the test plan:

- Review the exposed interfaces and components of the BR-GW
- Define the features that need to be tested
- Development of the test cases
- Execution of the test cases
- Detailed report of the testing

3.1.1.3 Test Schedule

Tests	**Project Months**																												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
BR-GW messages test																														
BR-GW component test																														
BR-GW End-to-End test																														

3.1.2 E-SMIS Test

3.1.2.1 Functional Description

The European Security Monitoring and Information System (E-SMIS) together with several further instances distributed across Europe, namely the DE-SMIS instances, compose the pan-European Security Monitoring Centre (ESMC). By the interplay between DE-SMIS and E-SMIS, ESMC detects pattern related to cyper attacks. Please see D4.4[4] for more details.

3.1.2.2 Test Strategy

We test E-SMIS in two phases:

1. we resort to simulated data which serves as input for E-SMIS, and
2. if possible, we use real data provided by the trial sites to test E-SMIS.

Resorting to simulated data has the advantage that one can determine which parameter should be tested under which conditions. Hence, individual scenarios can be tested in a flexible and customized way. However, the drawback is that appropriate simulation tools have to be developed to produce test data. For each simulation, one implicitely makes assumption about the real world where one has to ensure that they picture the uses cases in an sufficient accurate way.

The E-SMIS component test will be performed at the P3 Energy lab.

3.1.2.3 Test Schedule

We will test the components in three separate drops, where each drop comprises more functionality than the previous one.

Tests	Project Months																												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
E-SMIS (simulated data)																														
E-SMIS (real data)																														

3.1.3 DE-SMIS Test

3.1.3.1 Functional Description

DE-SMIS interacts with the DSOSMC to detect patterns related to cyber-attacks at DSOs/TSOs level. Please see Deliverable 4.4 for more details about DE-SMIS.

3.1.3.2 Test Strategy

We resort to similar strategies as used for E-SMIS to test DE-SMIS:

1. we resort to simulated data which serves as input for DE-SMIS, and
2. if possible, we use real data provided by the trial sites to test DE-SMIS.

See Chapter 3.1.2.2 for details about the simulation strategy. All single component tests will be performed at the P3 Energy lab.

3.1.3.3 Test Schedule

We will test the component in three separate drops, where each drop comprises more functionality than the previous one.

Tests	Project Months																												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
DE-SMIS (simulated data)																														
DE-SMIS (real data)																														

3.2 Integration test: Pairwise integration

3.2.1 Test Planning for NORM and BR-GW

3.2.1.1 Test Strategy

The test strategy will be provided in the next version of D4.7

3.2.1.2 Time Schedule

Tests	Project Months																												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
First Release												■																		
Second Release																■														
Third Release																			■											

3.2.2 Testing planning for BR-GW – DSOSMC

3.2.2.1 Test Strategy

The test strategy will be provided in the next version of D4.7

3.2.2.2 Time Schedule

The time schedule proposed will be based upon three main releases that will enclose in an incremental way providing all the functionalities needed. The third release will be ready to be integrated in the entire solution.

Tests	Project Months																												
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
First Release												■																		
Second Release																■														
Third Release																						■								

3.2.3 Test Planning for ESMC

The pan-European Security Monitoring Centre (ESMC) consists of a central instance, namely the Security Monitoring and Information System (E-SMIS), and several further instances distributed across Europe, namely the DE-SMIS instances. The E-SMIS and the DE-SMIS work together to detect patterns related to cyber-attacks and to alert DSOs or TSOs about attacks. Please see Deliverable 4.4 for more details about ESMC. We first describe the test plan for the single components DE-SMIS and E-SMIS. Afterwards, we give the test plan for the component ESMC.

3.2.3.1 Test Strategy

Evaluating ESMC consists of testing the individual components DE-SMIS and E-SMIS (see Sections 3.1.2, 3.1.3) together as a pair. It comprises as well as the communication between them. We will perform a paired component test for ESMC by evaluating

1. several DE-SMIS instances,
2. one DE-SMIS instance and E-SMIS, and
3. several DE-SMIS instances and E-SMIS.

Like the testing of the individual components of DE-SMIS and E-SMIS, we will also resort to real and simulated data for evaluating their communication. The paired component test of ESMC will be performed at the P3 lab. Additionally, ESMC will be evaluated at four locations:

1. the trial site in Ireland,
2. the trial site in Romania,
3. the trial site in Italy, and
4. the laboratory at RWTH Aachen.

At the RWTH lab in Aachen, we plan to reproduce situations where the energy grid is under cyberattack. At the trial sites, we plan to establish a proof-of-concept of ESMC in the field to show its working principles under real conditions. For that, we will define specific test cases for each trial site. Until now, the exact dates for the trial site experiments are not fixed yet.

3.2.3.2 Time Schedule

We will test ESMC in three separate drops at the P3 lab. Each drop will have more functionalities than the previous one. We will resort to using simulated and real data (second row). Moreover, we will use one or several DE-SMIS instances with or without E-SMIS (see row 1-3 and row 4-6, respectively).

	simulated data (S) or real data (R)																													
Tests		**Project Months**																												
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Several DE-SMIS	S																													
One DE-SMIS & E-SMIS	S																													
Several DE-SMIS & E-SMIS	S																													
Several DE-SMIS	R																													
One DE-SMIS & E-SMIS	R																													
Several DE-SMIS & E-SMIS	R																													

3.3 Integration of success security monitoring solution

The plan for the pair-wise integration of components has been described in Ch. 3.2 above. In this chapter, a time frame plan for the release of all the functionalities will be presented. The entire success solution points towards the real implementation in the pilot sites. Integration time plan is adjusted to fit the required MS9.

At the end of M20 the trial sites must be ready to implement the actual success solution. For this reason, the M13 is the date for first drop of preliminary integrated solution and M18 is the date for the first drop of the full integrated solution needed in M20 to build the pilot sites. The M23 release will be the final drop of the entire solution.

3.3.1 Interaction between ESMC and DSOSMC

3.3.1.1 Test Strategy

The test strategy details will be provided in the next version of D4.7

3.3.1.2 Time schedule

The entire SUCCESS solution will be tested in the pilot sites. Integration is adjusted for this by requiring MS9 for trial site to begin to integrate the solution into real infrastracture.

Tests	**Project Months**																													
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
First Release																														
Second Release																														
Third Release																														

4. Certification

This section describes the process and the necessary elements thereof that will need to be followed for a future certification of the SUCCESS components that will be developed in WP4. In this deliverable, a general approach to the certification process, which can also be used for the certification within Task 3.6 - *Certification feature catalogue, feature specifications and test plans*, as well as specific examples indicating the SUCCESS components and their functionalities are provided. The technical outputs of this deliverable and of its subsequent versions, along with the

respective ones from Task 3.6, will be provided to WP6 for the development of the Certification Centre. The certification process will cover all requirements specified for each device or element, including the individual and the integrated operation. In this chapter, the focus is set on security aspects, given that the project mainly concentrates on securing the smart grid, and interoperability aspects, regarding the communication of the SUCCESS devices and elements with each other and with external stakeholders, as depicted in Figure 2. In the figure, the interfaces have generic identifiers, which should not be confused with the interfaces described in [4].

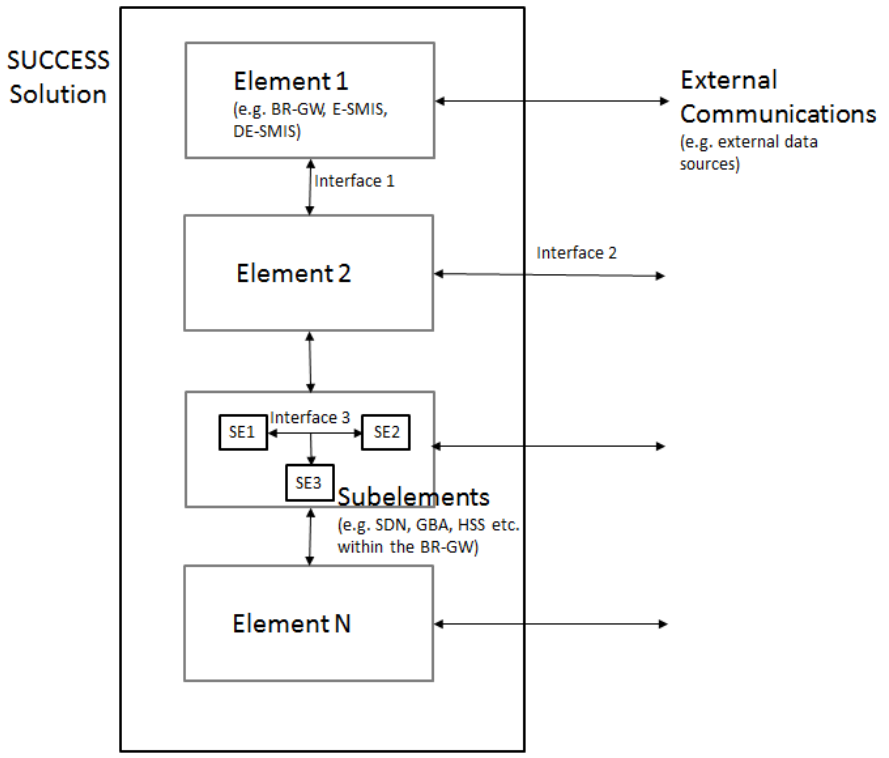

Figure 2: SUCCESS Solution

4.1 Approach to Certification Process

4.1.1 Significance of Certification

Certification is the confirmation from a competent authority that a device or an element fulfils specific functional properties. Certification is applied in most commercial products, since it is a formal statement that the products operate as expected.

In the future, commercial devices from different manufacturers are expected to be integrated into the SUCCESS solution. To achieve a satisfying level of security and proper interoperability among the different devices, standardization of necessary features and functions needs to be done, which will gradually conclude on the respective set of minimum (mandatory) and other additional (optional) requirements valid for each point in time (including backward and forward compatibility issues). These requirements ensure that a device or element provides the security that is needed within the SUCCESS solution. They also ensure that it can be considered as a functional entity, with functional and operational interfaces that are consistent over the implementations of different manufacturers and the models, enabling seamless interoperability and compliance with standards to verify the full (or where it applies partial) availability of the respective features.

4.1.2 Overview of the Elements in the Certification Process

The certification of a device is a thorough procedure that should take into consideration the behaviour of the device in a variety of environments and use cases. Therefore, several elements with specific terminology have been developed to describe the abovementioned parameters. These elements are concentrated in the following table:

Table 1 – Elements in the Certification Process

Term	Definition
Device Class	Group consisting of devices that have the same functionalities and may come from different manufacturers.
Operation Mode	Different states that may be available in a device for different use cases.
Functional Group	Functionalities that are covered within the device classes.
Feature	Simple functionalities that comprise the functional groups.
Profile	A detailed document describing a feature.
Test Plan	A document describing various tests for the certification of a feature.
Reference	A standard that a feature should conform to. It is usually a part of the Profile.
Interfaces	A list with the interfaces relevant to a feature.
Requirements Table	A list including all functional groups of a device class.

4.1.3 Steps for the Certification

A significant step in setting up the process on certification for the overall infrastructure is the specification of the devices under test. The selection and design of the utilized components that are included in the scope of the process described within this and the subsequent relevant deliverables are naturally based on the functionalities (functional groups) that will be addressed in the project. The complete specification of the components requires the specification of the necessary interfaces at the interoperability level desired and the definition of test plans (for respectively specified test cases) which can be used for feature verification.

Certification is preceded by the analysis of the features for the use cases, the tests and the validation. The definition of the components and their features is partially given in Ch. 3 and will be completed in later versions of the deliverables. They will thus feed the certification process, since the components and their features need to be determined first. Further steps may be required at certification level, so that each feature is examined for a broader list of test cases. The features are registered in a catalogue (feature catalogue), which are subsequently matched to the respective test plans. The structure including the feature catalogue, the functional groups and the devices under test is called certification matrix and provides an overview of the entire certification process relationships that need to be respected.

The development procedure of this matrix is depicted in Figure 3 and includes four steps. The development process is iterative and the results thereof need to be aligned with the respective stakeholder groups, so the four steps need to be revisited many times during the development process. The four steps are as follows:

1. Creation of a list with the functional groups that are necessary or auxiliary for achieving the SUCCESS objectives. A functional group describes an activity that will be conducted at one or more levels of the SUCCESS architecture.
2. Definition of the device classes that will cover the required functional groups of Step 1 and of their possible operations for the different conditions (operation modes). For each operation mode, the number and the necessity of the functional groups that will be fulfilled by the device class may differ. Therefore, the certification matrix must define explicitly which functional groups are included in the respective device class for each operation mode. A functional group may be deemed mandatory, if it is essential for the normal operation of the device class, or optional, if it merely increases the value, capabilities or user-friendliness of the component. The manufacturer of a product must include all mandatory functional groups of the corresponding device class and has the choice of adding any of the optional functional groups towards rendering the product more efficient or more competitive. Furthermore, a new device class can emerge through a combination of functional groups by the manufacturer, so that its product can better satisfy the operational requirements it has been designed for. The Requirements Tables of the device classes are completed at this step.

3. Decomposition of each functional group into features. A feature may belong to several functional groups, either as mandatory or as optional, following the same rationale as in Step 2. A certification of a product is granted for a functional group upon successful tests of every mandatory feature. If the product fails a single test, it cannot acquire the certification.
4. Detailed analysis of the features. The analysis includes a Profile, the interfaces and a Test Plan for each feature.
    a. A Profile describes thoroughly the feature and is normally based on existing standards and tests from internationally recognised organisations, such as ISO, IEC and ETSI. When a standard cannot be explicitly applied on a particular feature and fully describe its functionalities, the additional requirements are complemented or a new standard may be developed.
    b. Several interactions with other devices may emerge for some features. These interactions are described through the list of the interfaces.
    c. A Test Plan is created to test the feature in ideally every possible case that may occur during the operation of a device. In practice, the different stakeholder groups may conclude that it is sufficient to treat specific (critical) cases. The Test Plan ensures that the testing and certification of all components follow a standardised, transparent and reproducible procedure. Each device or element undergoes a number of tests for the features included in its Requirements Table and the certification is achieved upon successful completion of the tests by a competent authority.

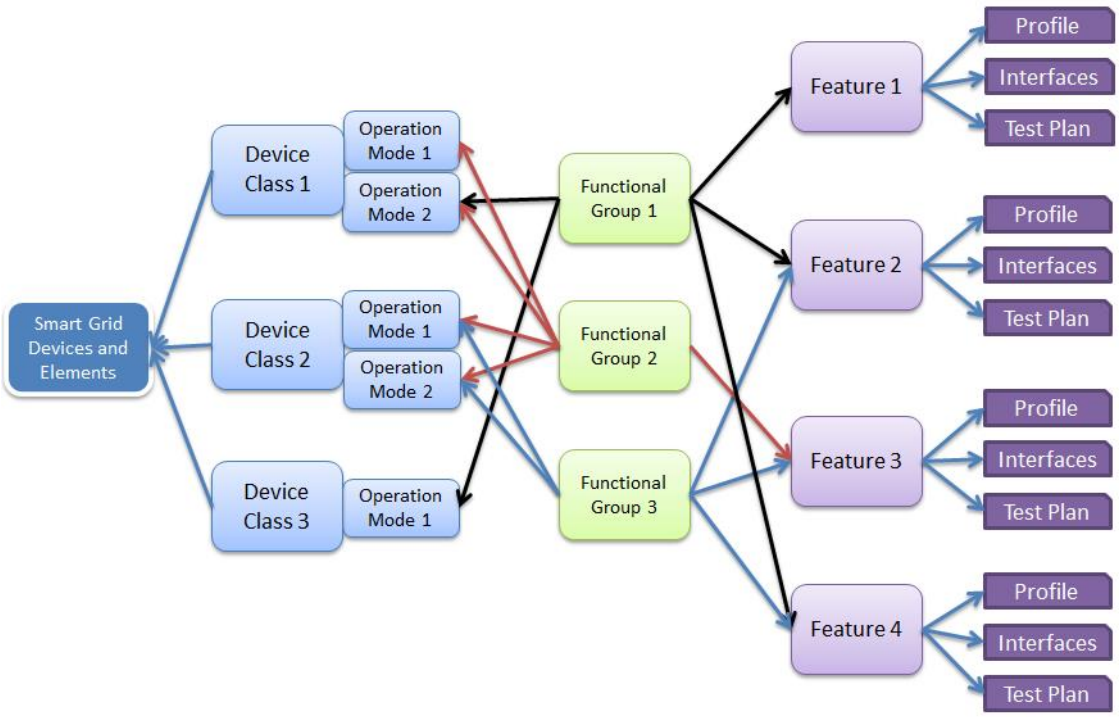

Figure 3: Certification Matrix Development

4.2 Feature Catalogue and Certification Matrix of the SUCCESS Components

4.2.1 Functional Groups

The main objective of SUCCESS is the implementation of the concepts of security, resilience and survivability by design in the Smart Grid. These concepts deduce on the functionalities that need to be introduced in the project and fulfilled by the SUCCESS components. Examples of functional groups can be the encryption of data, the creation of redundant communication paths, the real-time transmission and processing of data and remote control. At every level of the SUCCESS

solution, device classes will be defined to cover the functional requirements mentioned in the functional group list. The functional groups can be either mandatory or optional for a device class, as described in Section 4.1, based on the requirements specified for each operation mode of the device class.

4.2.2 Device Classes

The components described in WP4 for the SUCCESS Security Monitoring Solution, have been selected and will be further tailored to serve the fundamental and supplementary needs of SUCCESS. Therefore, the:

- NORM,
- BR-GW,
- DSOSMC,
- DE-SMIS and
- E-SMIS

are the device classes, to which one or more functional groups correspond. The operation modes have not yet been fully defined and will be formulated in the next versions of the deliverable, in accordance with the use cases of WP2, WP3 and WP4, which also describe the different external conditions, frameworks and device states from a conceptual view and in the real-world implementation. Table 2 in Section 4.2.3 includes the device classes and operation modes that can be concluded at this stage of the project.

4.2.3 Features

The features for the device classes utilized in SUCCESS solution can be partially extracted from their functionalities, as they are described in deliverables D3.10 [7] and D4.4 [4]. They will be fully determined in the later versions of the deliverable, since the functional groups have not been explicitly defined so far. They will cover all desired security and interoperability aspects that have been addressed within SUCCESS. In Table 2 the initial results from the analysis of the device classes, mentioned as functionalities, are presented. These functionalities will be considered either as features or as functional groups in later versions, depending on whether they can be further analysed into smaller individual entities.

Table 2 – Devices classes

Device Class	Operation Modes	Functionalities
NORM	NORM has the same operational mode in all situations	• Communicate with HAN • Communicate with public networks through the internet (secure communication through OpenVPN) with at least the following actors: DS-SMC (for monitoring cyber-security aspects), Administrator (for administrating different settings), DSO (for real-time data and for collecting billing data, where it has this role), other actors which have the right to access the NORM SMG • Measure consumer/prosumer data from the energy meter • Measure grid-related data
BR-GW	Different operation modes regarding routing, security and bandwidth management, depending on real-time demands in the network and application requirements	SDN: • Control flow of network traffic • Dynamic configuration of the network DCS: • Perform data integrity check • Eliminate security threats caused by data manipulation • Use Keyless Signature • Compute hash value from received data • Notify DSOSMC NMF: • Detect network threats • Inspect packets

		• Notify DSOSMC • Block traffic originating from malfunctioning node
DSOSMC	Different time steps and averaging periods for the data collection, depending on the application needs	• Collect data from NORMs • Perform selection of data • Pre-process the selected data • Alert and trigger proper strategies/countermeasures • Provide aggregated security information to the Utilities, in the form of KPIs • Send information to other DSOSMC components • Send information to DE-SMIS <u>Countermeasures Extraction Tool:</u> • Provide list of possible countermeasures <u>Semantically Enhanced Countermeasures Module:</u> • Select the best countermeasure • Populate the Countermeasures Knowledge Database • Show list of countermeasure in a dashboard
ESMIS	• Normal operation: share only attack patterns data • Fall-back operation: share all anonymised data	• Receive data from DSOSMC • Receive data from other internal sources • Extract new meaning and information about the system by using data mining algorithms on the received data • Make the collected data anonymous • Receive data from external data sources • Search for unexpected and significant patterns • Precisely visualise the results for human-machine interactions • Notify responsible authorities

4.2.4 Test Plans

A thorough description of the respective Profile and a Test Plan will follow. It is important to note that the tests planned for the validation of the SUCCESS components within this WP may have a narrower scope than the feature Test Plans for certification; however, they will provide an initial concept for the development of the certification plans. Therefore, certification Test Plans may result from the aggregation and integration of all validation test plans developed within WP4. Furthermore, any additional test cases that may be excluded from the validation test plans may be also complemented.

4.2.5 Certification Authority

The testing will be conducted by an laboratory that will be designated by a competent authority. This authority will also grant the certification. The scope of this deliverable and of the respective in WP3 is only to provide technical input and more detailed information on the laboratory and the authority will be presented in WP6.

5. References

[1] SUCCESS, “Deliverable D4.7 : Integration and Validation Plan. Test and certification specifications v1,” 2017.

[2] SUCCESS, “Deliverable D4.8 : Integration and Validation Plan. Test and certification specifications v2,” 2017.

[3] SUCCESS, “Deliverable D4.9 : Integration and Validation Plan. Test and certification specifications v3,” 2018.

[4] SUCCESS “Deliverable D4.4: Description of Available Components for SW Functions, Infrastructure and Related Documentation, V1”, 2017

[5] SUCCESS “Deliverable D5.1: Trial site planning”, 2017

[6] Ammann, P., & Offutt, J. (2016). *Introduction to software testing*. Cambridge University Press.

[7] SUCCESS, “Deliverable D3.10 : Integration and Validation Plan. Test and certification specifications v1.0” 2017.

6. List of Abbreviations

BR-GW	Breakout Gateway
CA	Certificate Authority
DCS	Data Centric Security
DEMS	Decentralised Energy Management System
DE-SMIS	Distributed instance of European Security Monitoring and Information System
DSO	Distribution System Operator
DSOSMC	DSO Security Monitoring Centre
ESMC	Pan-European Security Monitoring Centre
E-SMIS	Security Monitoring and Information System
NAN	Neighbourhood Area Network
NORM	New-generation Open Real-time Smart Meter
NMF	Network Monitoring Function
PMU	Phasor Measurement Unit
SDN	Software Defined Networking