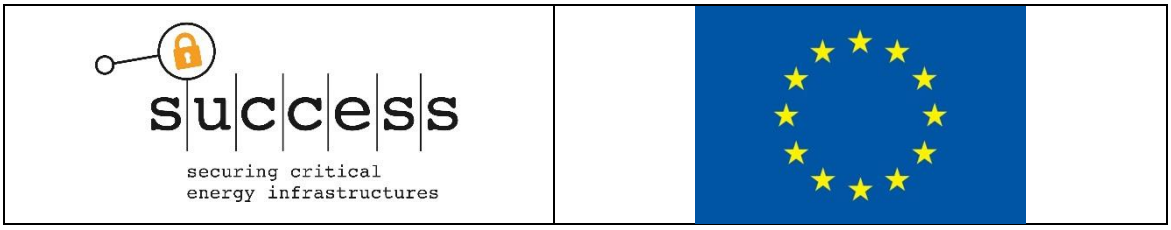
Ref. Ares(2017)3837424 - 31/07/2017



SUCCESS

D3.11

Integration and Validation Plan. Test and certification specifications, V2

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 July 2017
Actual Delivery Date:	31 July 2017
Contributors:	ENG, P3C, ISMB, RWTH, SYN
Workpackage:	WP3 - Securing Smart Devices
Security:	PU
Nature:	R
Version:	1.0
Total number of pages:	35

Abstract:
This deliverable presents the outcome of the SUCCESS consortium developments in the context of tasks T3.5 and T3.6 and pertains to the integration of components of WP3, embodying the interfacing between the DSOSMC, NORM and the Distribution Grid. Moreover, this report outlines the necessary processes and the associated methodology towards integrating and testing, at functional level, between WP3 components within the SUCCESS Security Monitoring Solution.

Keyword list:

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

Disclaimer:

All information provided reflects the status of the SUCCESS project at the time of writing and may be subject to change.

Executive Summary

This deliverable documents the current status of the Integration and Validation Plan. Test and certification specifications.

It updates D3.10, providing more details of the plan for integration of the NORM and the DSOSMC.

This new version is intended to use also part of the results reported in D3.13 for the certification methodology, i.e. the features for pairwise integration testing build on the collected features for single components testing.

Compared to the old version D3.10 of this deliverable, in this new version D3.11 the NORM and DSOSMC are meant to work together from the features point of view and the outcome of this approach is to provide a set of detailed test cases that will be executed and validated in D3.12 allowing both a single component validation and pairwise integration. It useful to keep in mind that following the same approach, the complete integration and validation of SUCCESS Security Monitoring solution will be realized in D4.8 and D4.9.

Document History

Date	Revision	Comment	Author/Editor	Affiliation
16-06-2017	V0	TOC	Antonello Corsi	ENG
13-07-2017	V0.1	Initial input	Antonello Corsi	ENG
17-07-2017	V0.2	Updated TOC	Antonello Corsi	ENG
18-07-2017	V0.3	Deliverable review, general updates, updated Pairwise integration details	Artemis Voulkidis	SYN
19-07-2017	V0.4	Test cases first round check	Panagiotis Paschalidis	P3C
20-07-2017	V0.5	Updated end-to-end tests	Artemis Voulkidis	SYN
21-07-2017	V0.6	Check on end to end tests	mikhail simonov	ISMB
22-07-2017	V0.7	Update and check on content	Padraic McKeever	RWTH
24-07-2017	V0.8	Further DSOSMC and NORM pairwise test definition	Antonello Corsi	ENG
26-07-2017	V0.9	Document review	Artemis Voulkidis	SYN
31-07-2017	V1.0	Addressing comments and make deliverable ready for review	Giampaolo Fiorentino	ENG

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
SYNELIXIS (SYN)		
	Artemis Voulkidis	voulkidis@synelixis.com
Rheinisch-Westfaelische Technische Hochschule Aachen(RWTH)		
	Padraic McKeever	PMcKeever@eonerc.rwth-aachen.de
ISMB		
	Mikhail Simonov	simonov@ismb.it

Table of Contents

List of Tables

1. Introduction

1.1 Scope of this Deliverable

This document composes the second version of the test and validation plan for integrating and testing components in the SUCCESS Security Monitoring solution that pertain to monitoring and controlling Neighbourhood Area Network (NaN) assets, namely the Next-generation Open Real-time Meter (NORM) and Distribution Service Operator Security Monitoring Centre (DSOSMC). It is a natural extension of D3.10 [1] describing the main interactions between the two components in terms of expected behaviour and protocols for communication. DSOSMC and NORM constitute the local part of the SUCCESS solution that act as first security layer. The document focuses on the updates performed in the entire integration and validation plan with respect to [1] and follows the guidelines framed in the structure described in D3.13 [2].

The process for integrating and testing both NORM and DSOSMC is described, including a description of how to test the implemented system against a set of features collected and described by D3.13. As in the case of the latter, this document is largely based on the definition of sets of features that used to define integration tests, examining the operation of DSOSMC and NORM, combined, from both a logical and functional point of view.

In this deliverable, the objectives pursued are:

- To provide a plan for certification and integration based on the features documented in D3.13, extending the integration testing plan already defined in D3.10 based on the updated functionalities described in D4.4, D4.5 and D3.5;
- To provide the guidelines for integrated WP3 components testing;
- To validate that the DSOSMC and the NORM are able to properly interwork in more complex, yet real-life scenarios.

1.2 Intended audience

The SUCCESS project partners are directly interested in this document, since the coordinated setting of the testing procedures of the integrated features of the SUCCESS Security Monitoring Solution and its harmonization with the certification processes will safeguard the activities of the project, leading to a smooth trial-sites operation phase.

Apart from the project partners, the present document could be of potential interest to the following Smart Grid actors:

DSOs	DSOs could be interested in checking whether their current equipment satisfies the advanced security specifications and test cases presented in this document, implicitly assessing the flexibility and security status of their own systems.
Smart grid assets manufacturers	They would be interested in checking whether their products would be ready to support next-generation, SUCCESS security certified smart grid architectures and platforms holding security and privacy by design as top priorities.
Smart metering products manufacturers	NORM, one of SUCCESS' primary offerings, is a flexible combination of an open hardware platform (Raspberry PI3 [3]) coupled with advanced software and hardware services to support modern and legacy smart meters. Certification against the identified integration requirements would imply compliance to a large range of smart meters and services, as well as to the security guidelines as identified by the SUCCESS security experts.

1.3 How to read this document

Since this deliverable is an update of D3.10 [1], a good understanding of it's content is required before the reader reads this document. As the present document targets the identification of

test cases for Neighbourhood area Network (NaN) assets that fare of interest to SUCCESS, for reasons of clarity, the reader needs to have a basic understanding of the technologies and naming adopted in SUCCESS. The starting point for the interested reader should be deliverable D4.2 [4], which presents the SUCCESS Security Monitoring Solution architecture and offers a high-level introduction on the SUCCESS project mission, goals and approach. Further, another fundamental resource is deliverable D3.13 [2], where the individual testing activities and specifications are documented. D3.13 also acts as the basis of the integrated features definitions.

In case a deeper understanding of the features and technical specifications is required by the reader, we suggest that D3.4 [5] and D3.5 [6] should be read, both offering insights about the actual design and implementation details of the DSOSMC. Knowledge of itheir contents is necessary to be able to follow the discussion related to testing the SUCCESS reference DSOSMC design and requirements. The same holds for D3.7, which provides information related to the NORM specifications. Lastly, a good understanding of D1.2 [4] is required to understand the core threats against which the SUCCESS Security Monitoring Solution intends to offer protection, documented as the features described in the aforementioned deliverables.

Having covered the core concepts of the SUCCESS Security Monitoring Solution, this document should be read linearly, Annex A offers an overview of the identified test cases.

1.4 Relation to other project activities

This deliverable is directly linked with all the activities performed by the SUCCESS consortium in the context of securing the Smart Grid at Neighbourhood area Network (NaN) level, hence the activities of WP3. In this context, and as the core focus of the deliverable is to document the testing activities for all relevant integrated components (as opposed to deliverable D3.13 [2]), the activities carried out in the following SUCCESS project tasks:

- Task 3.3, entitled “DSO Security Monitoring Centre”, since in this document the test cases for the components composing the overall DSOSMC will be detailed;
- Task 3.4, entitled “Development of next generation Smart Meter for trials (NORM)”, since in this document the test cases for the components composing the NORM will be detailed;
- Task 3.5, entitled “Information Security Management Integration and Testing”, since the integration planning and testing is directly linked to the individual components testing procedures and time schedule;
- Task 3.6, entitled “Certification feature catalogue, feature specifications and test plans”, since they share context with regards to both feature catalogue and specifications and test plans.

Moreover, under a certification perspective, this deliverable is loosely coupled with the certification centre activities carried out in Task 6.2.

Lastly, it should be highlighted that the methodology and structure presented will be also adopted by the relevant work stream of securing the smart infrastructures in the context of the Integration, Testing and certification activities, documented in D4.8 [7] and D4.9 [8].

2. Integration and validation test and certification methodology

Building on the output of deliverables D3.10 [1] and D3.13 [2], yet under an integrated functionality perspective, this deliverable largely follows the methodology documented in [2]. Integrated validation and testing will be pursued in two directions, namely on the basis of:

1. pairwise, interface-level testing among the various components, effectively performing in a real environment the individual tests described in [2] (many times assisted by simulated component functionality);
2. integrated testing among the various components, essentially validating the logical functionality of the SUCCESS NaN- and DSO-level developments, covering the co-existence of NORM and DSOSMC.

With respect to the second point, since the focus of this deliverable is put on the NaN level assets of the Smart Energy Grid (NORM, in particular), and the security infrastructure managing their security context (in the context of the SUCCESS Security Monitoring Solution, the DSOSMC), only the relevant functionalities are being discussed, leaving the discussion on the integration and validation test and certification methodology related to DSOSMC and the rest of the SUCCESS components (excluding NORM) to deliverables D4.8 [7] and D4.9 [8].

With respect to pairwise testing, this may include testing:

1. the interfacing of sub-components inside the same component (e.g. testing that the DSOSMC Monitoring component is able to actually communicate with DSOSMC Analytics component [5], etc.) or
2. the interfacing of specific components residing in NORM and DSOSMC (e.g. test that the local NORM Physically Unclonable Function agent is able to properly communicate with an instance of the DSOSMC Key Management Module – see [2], [6], [9]).

The relevant features for the pairwise testing have been documented in [1] and are, therefore, left out of the analysis of the present document.

With respect to integrated testing, this pertains to validating that the logic governing a logically and realistically-framed scenario covering end-to-end functionalities is properly implemented. Evidently, the integrated testing should consider scenarios where the maximum possible set of independent functionalities is tested, spanning operations from both NORM and DSOSMC components.

2.1 Adopted methodology

The methodology for defining and documenting the integration and validation test and certification procedures will follow the pattern extensively documented in D3.13 [2], naturally focusing on an integrated approach rather than a stand-alone, component-sandboxed perspective followed by [2].

Following [1] and [2], the test and certification specifications will follow a step-wise approach composed of eight steps as follows:

1. Identification of integrated smart grid components to be tested
2. Grouping of functional features
3. Identification of functional features of identified, integrated components
4. Mapping of the integrated components' functional features to technical specifications
5. Definition of test templates
6. Specification of test cases
7. Define test and certification time schedule
8. Test cases validation

It should be highlighted that step 5 pertaining to the definition of the test templates has already been conducted in the context of [1]. However the slightly updated templates of [2] will be adopted in this deliverable. Similarly, the tables presenting the technical specifications in this deliverable follow the structure of the templates adopted in [2].

2.2 Application of the methodology to SUCCESS developments

2.2.1 Identification of integrated smart grid components to be tested

In the context of integration and validation testing and certification specification processes that this document addresses, the integrated smart grid components of interest are the DSOSMC and the NORM. For naming reasons, the integrated system referring to their coordinated interfacing is notated as *DSNM*[1].

2.2.2 Grouping of functional features

The groups of functional features have been extensively documented in [2] (Table 4) and are tabulated below for reasons of document clarity. Note that an additional group has been introduced, namely G10, aggregating features related to end-to-end functionality, spanning functional features from multiple groups.

Table 1: SUCCESS groups of functional features

ID	Title	Description
G1	AAA	Authentication, authorization and accounting features. Though not all of these may be supported (e.g. accounting), mechanisms to ensure that unauthorized access to any kind of service or data is prohibited should be implemented.
G2	Streams protection	Features related to the protection of the data residing within a shared medium, be it a transmission link or a physical storage device (e.g. a hard disk).
G3	Metering services	As the core concept of SUCCESS Security Monitoring Solution is based on the continuous monitoring of non-personal, network data such as voltage, frequency, etc., the existence of metering services is considered necessary. In this group, such services residing at devices level are classified.
G4	State monitoring	This group pertains to the non-device oriented counterparts of the metering services, namely systems that can evaluate the metering services output and assess the security status of the grid.
G5	Asset management	Features related to managing the behaviour of various assets of the Smart Grid, spanning from devices at NaN level up to pan-European security monitoring entities.
G6	Time synchronization	As SUCCESS evangelizes that the large-scale use of PMUs is beneficial to the security monitoring processes, this group is related to ensuring that proper services for time synchronization are deployed at PMU level.
G7	Threats management	Features related to identifying and assessing threats. This group includes the local security agent of NORM, as well as the threat identification processes of the DSOSMC and the E-SMIS (though the latter is out of the context of this document)
G8	Countermeasures management	This group includes the broad countermeasures-related features. In SUCCESS, countermeasures are meant to be managed at DSOSMC and ESMC level.
G9	User Interaction	This group includes features related to handling the control of a component behaviour to the component end-user through user-friendly interfaces.
G10	End-to-end	Generic group referring to functional features referring to multiple groups and features. Should be used for rationality and overall functionality checking only.

[1] DSNM stands for DSOSMC ↔ NORM. Although a more verbose naming would generally improve features self-documentation level, the DSNM notation has been adopted for reasons of document clarity and brevity.

2.2.3 Identification of functional features of identified, integrated components

In the framework of two-level testing and certification specification of this document, the interface-level pairwise functional features are defined as the fusion of the individual component features documented in [2], granted that no emulating services are involved but, rather, the actual implemented component instantiations. The relevant (fused) features are tabulated below.

Table 2: DSNM Features

DSNM feature ID	DSNM feature name	§
DSNM:G1:F1	Authentication of Physically Unclonable Functions (PUF)-enabled NORM devices	2.2.3.1
DSNM:G1:F2	Periodic update of the active challenge-response pair (CRP) of PUF-enabled NORM devices	2.2.3.2
DSNM:G2:F1	Encryption and decryption of reported data	2.2.3.3
DSNM:G2:F2	Channel encryption	2.2.3.4
DSNM:G3:F1	Integrated NORM metrology services	2.2.3.5
DSNM:G7:F1	Support for standard security services	2.2.3.6
DSNM:G10:F1	Mitigation of incidents implying compromise of the SMM or the low-cost PMU module of NORM devices	2.2.3.7
DSNM:G10:F2	Mitigation of incidents implying malware/virus infection on the NORM devices	2.2.3.8
DSNM:G10:F3	Mitigation of incidents where remote software attestation fails	2.2.3.9
DSNM:G10:F4	Mitigation of incidents where remote hardware attestation fails	2.2.3.10
DSNM:G10:F5	Mitigation of incidents where firewall configuration is unexpected	2.2.3.11
DSNM:G10:F6	Mitigation of incidents where NORM devices are unavailable	2.2.3.12
DSNM:G10:F7	Mitigation of incidents where NORM devices cannot authorize themselves	2.2.3.13

In the following subsections, the descriptions of the integrated DSNM functional features mentioned in Table 2 are provided. Not that for the end-to-end features, the Incident-Countermeasure ID as provided in deliverable D4.5 [10] are also provided, wherever possible.

2.2.3.1 Feature DSNM:G1:F1 – Authentication of PUF-enabled NORM devices

Base Features: DSOSMC:G1:F1, NORM:G1:F1
Feature Type: Pairwise

Consolidating the functional features DSOSMC:G1:F1 and NORM:G1:F1, this integrated functional features refers to the ability of the DSOSMC and the NORM to interwork with a view to leverage on the hardware security capabilities granted to NORM by the PUF module [9]. This interworking includes the ability of DSOSMC to i) bootstrap NORM devices, ii) manage the CRPs of the supported NORM devices and iii) verify their authenticity effectively implementing NORMs authentication, authorization and accounting (AAA).

2.2.3.2 Feature DSNM:G1:F2 – Periodic update of the active CRP of PUF-enabled NORM devices

Base Features: DSOSMC:G1:F2, NORM:G1:F1
Feature Type: Pairwise

As per DSOSMC:G1:F2, the DSOSMC should be able to periodically or on-demand update the active CPR of the NORM devices supported by the DSOSMC instance.

2.2.3.3 Feature DSNM:G2:F1 – Encryption and decryption of reported data

Base Features: DSOSMC:G2:F1, NORM:G2:F1
Feature Type: Pairwise

As reported in [5], [9] and [2], the NORM devices should be able to send encrypted data to the DSOSMC as a further security measure on top of the communication channel encryption (see §2.2.3.4 for details). The encryption of the data should be performed by the PUF hardware security module integrated in the NORM, whereas the decryption of the data should be performed on the DSOSMC side (with the help of the KMM).

2.2.3.4 Feature DSNM:G2:F2 – Channel encryption

Base Features: NORM:G2:F5
Feature Type: Pairwise

The communications between the NORMs and the entities receiving the measured data (e.g. metrology, PMU-related, configuration etc.) should be performed over encrypted channels to ensure that the communications cannot be overheard by threat agents applying man-in-the-middle or eavesdropping attacks [11]. This feature, together with DSNM:G2:F1 would ensure that the SUCCESS Security Monitoring Solution features 2-level encryption on the devices-reported data streams.

2.2.3.5 Feature DSNM:G3:F1 – Integrated NORM metrology services

Base Features: DSOSMC:G2:F1, DSOSMC:G4:F1, NORM:G2:F1, NORM:G2:F3, NORM:G2:F4, NORM:G3:F1, NORM:G3:F2
Feature Type: Pairwise, End to end depending on the configuration

A NORM device should be able to report to the DSOSMC (possibly other actors as well, depending on the currently active policy for data reporting [9]) an encrypted set of meaningful measurements originating from either the integrated Smart Meter (metrology data) or the integrated low-cost PMU. On the other side, the DSOSMC should be in the position to, first, decode the data (see §2.2.3.3), then properly handle them (this includes data pre-processing and storage).

2.2.3.6 Feature DSNM:G7:F1 – Support for standard security services

Base Features: DSOSMC:G7:F1, NORM:G7:F2, NORM:G7:F3, NORM:G7:F4, NORM:G7:F5
Feature Type: Pairwise

The NORMs should expose interfaces that make feasible their remote security attestation by the DSOSMC services. These security attestation capabilities should guarantee that the DSOSMC is able to:

- Retrieve information or notifications about the integrity of the software deployed on each NORM (NORM:G7:F2);
- Retrieve information or notifications about the hardware integrity of the NORM per se (NORM:G7:F3);
- Retrieve information or notifications about the antivirus software activity running on the NORM devices (NORM:G7:F4);
- Assess and/or retrieve information or notifications about the security status of the firewall running on the NORM devices (NORM:G7:F5);
- Retrieve the log file of the NORM security services.

This data should be used by the DSOSMC Analytics module (see [5], [6] for details) to derive the security status of each supported NORM device.

2.2.3.7 Feature DSNM:G10:F1 – Mitigation of incidents implying compromise of the SMM or the low-cost PMU module of NORM devices

Base Features: DSMN:G1, DSMN:G2, DSMN:G3, DSMN:G7, DSOSMC:G4, DSOSMC:G7, DSOSMC:G8, NORM:G3
Feature Type: End to end
Incident ID: N/A

The DSOSMC should be in a position to understand that a certain set of NORMs have been compromised, by means of exploiting features DSMN:G1, DSMN:G2, DSMN:G3, DSMN:G7 as well by means of applying advanced monitoring and analytics (DSOSMC:G4, DSOSMC:G7) and algorithmic processes to detect situations that might imply the emergence of a security incident, as described in [10], pertaining to manipulation of either the SMM or the low-cost PMU (abnormal measurements activity). Upon detection of such a situation, the DSOSMC should select the appropriate countermeasures strategy to mitigate the identified threat (DSOSMC:G8), e.g. by temporarily disconnecting the meter.

2.2.3.8 Feature DSNM:G10:F2 – Mitigation of incidents implying malware/virus infection on the NORM devices

Base Features: DSNM:G7:F1, NORM:G7:F4
Feature Type: End to end
Incident ID: CS-4

The DSOSMC should be able to understand that a certain set of NORMs has been compromised by malware, rootkits or viruses, by means of exploiting features DSMN:G7:F1 and all features falling under NORM:G7:F4. Upon detection of such a situation, the DSOSMC should select the appropriate countermeasures strategy to mitigate the identified threat (DSOSMC:G8), e.g. by enforcing periodic antimalware, anti-rootkit and antivirus checks and instructing the relevant software signatures updates more frequently, until the problem is resolved. This feature relates to Incident-Countermeasure CS-4 as defined in [10].

2.2.3.9 Feature DSNM:G10:F3 – Mitigation of incidents where remote software attestation fails

Base Features: DSNM:G7:F1, NORM:G7:F2
Feature Type: End to end
Incident ID: CS-2

The NORM has local software attestation capabilities (NORM:G7:F2) which should be exposed to the DSOSMC either in the form of an API, or in the form of a report, so that the latter may act as deemed appropriate (DSNM:G7:F1). In case the software attestation fails, the DSOSMC should send a disconnection command to the NORM, then either try to re-flash the correct software image to the NORM filesystem, or send a physical maintenance unit to do it. In all cases, the NORM authentication credentials (active CRP) should be reset to ensure secure and private communications. This feature relates to Incident-Countermeasure CS-2 as defined in [10].

2.2.3.10 Feature DSNM:G10:F4 – Mitigation of incidents where remote hardware attestation fails

Base Features: DSNM:G7:F1, NORM:G7:F3
Feature Type: End to end
Incident ID: PS-2

Similar to DSNM:G10:F3, but referring to hardware attestation (e.g. case opening or equipment replacement). As the NORM features mechanisms (implemented by the local security agent, feature NORM:G7:F3) to identify its hardware configuration status, this information should be acknowledged to the DSOSMC. In case such an unplanned hardware configuration change is detected, the DSOSMC should send a disconnection command to the NORM, then send a physical maintenance unit to check and repair the configuration of the compromised NORM device(s). In all cases, the NORM authentication credentials (active CRP) should be reset to ensure secure and private communications. This feature relates to Incident-Countermeasure PS-2 as defined in [10].

2.2.3.11 Feature DSNM:G10:F5 – Mitigation of incidents where firewall configuration is unexpected

Base Features: DSNM:G7:F1, NORM:G7:F5
Feature Type: End to end

Incident ID: N/A

Similar to DSNM:G10:F2, but referring to the status of the firewall of the NORM devices; since the NORM needs to integrate with the DSOSMC and other services and actors, several network ports would need to be open in order to allow the internal NORM services to communicate with the corresponding external services. In any case, the configuration of the firewall should be the same for all NORM devices. If a port scanning indicates that the default configuration has been altered (e.g. leaving more ports in a listening state), then a command to reset the firewall configuration should be sent to the NORM device(s).

2.2.3.12 Feature DSNM:G10:F6 – F

Base Features: DSNM:G7:F1, DSOSMC:G4:F1, DSOSMC:G7:F1
Feature Type: End to end
Incident ID: PS-3, PS-4, PS-5

There are multiple reasons why a NORM device is not available (namely direct communication with it is not possible), including communication links failure, power supply failure or other, unknown generic reason failure. In the case that a NORM device is found to be unreachable, then the DSOSMC, having acknowledged the issue, should send an alert to the DSO Security Staff through the Dashboard that a maintenance unit should be sent on-site to fix the issue. This feature relates to Incident-Countermeasure PS-3, PS-4 and PS-5 as defined in [10].

2.2.3.13 Feature DSNM:G10:F7 – Mitigating incidents where NORM devices cannot authorize themselves

Base Features: DSNM:G1, DSNMM:G2, DSNM:G7:F1, DSOSMC:G1, DSOSMC:G2, NORM:G1, NORM:G2
Feature Type: End to end
Incident ID: CS-3

This feature refers to cases where the validation of the NORM devices fails, or there emerge repeating decryption service failures, indicating that either the synchronization of the PUF component of the NORMs has been broken, or the PUF hardware security module has been compromised/replaced/broken. In every case, the DSOSMC services should be able to detect the issue and accordingly i) try to re-establish the authentication synchronization with the NORM by activating a new CRP or ii) send a maintenance unit to check the NORM physically. Note that in the case of NORM PUF compromise/replacement, this feature could fall back to DSNM:G10:F4. This feature relates to Incident-Countermeasure CS-3 as defined in [10].

3. Integrated DSOSMC and NORM testing and validation

3.1.1 Technical Specifications

The technical specifications of NORM and DSOSMC have been extensively documented in [2] and their presentation is omitted in this document for reasons of brevity. For DSNM, no further technical specification can be provided as the DSNM refers to the fusion of the functionalities of two actual components, without it offering new, additional functionality.

3.1.2 Test templates

The test template used for testing has been provided in [2] and will be adopted as such.

3.1.3 Test cases

3.1.3.1 Test cases for feature DSNM:G1:F1

Table 3: Test case DSNM:G1:F1:T1

Test ID	DSNM:G1:F1:T1		
Test Description	Test that the DSOSMC can bootstrap a PUF-enabled NORM, by registering sets of CRP.		
Test location	At the premises of SYN	**Partner**	SYN
Component	DSOSMC, NORM		
Features under test	DSNM:G1:F1		
Product requirement	The DSOSMC should be able to bootstrap a NORM device.		
Test environment	An active DSOSMC instance and a NORM device.		
Preparation	N/A		
Dependencies	N/A		
Steps	1. The NORM should send a message to the DSOSMC KMM indicating that it needs to be bootstrapped, specifying its ID; 2. The DSOSMC KMM sends a list of 5000 distinct challenges to the NORM; 3. NORM responds to the DSOSMC KMM with 5000 different response strings; 4. The KMM registers 5000 pairs of challenge-response strings in its challenge-response database.		
Pass criteria	5000 distinct challenge-response are stored in the challenge-response database of the KMM.		
Suspension criteria	N/A		

Table 4: Test case DSNM:G1:F1:T2

Test ID	DSNM:G1:F1:T2		
Test Description	Test that the DSOSMC KMM can identify a PUF-enabled NORM device.		
Test location	At the premises of SYN.	**Partner**	SYN
Component	DSOSMC, NORM		

Features under test	DSNM:G1:F1
Product requirement	The DSOSMC should be able to uniquely identify a NORM device.
Test environment	An active DSOSMC instance and at least two NORM devices.
Preparation	N/A
Dependencies	Test case DSNM:G1:F1:T1 should have been successfully executed right before this test, considering at least two NORM devices
Steps	1. The two NORM devices are fed with a set of active challenges, based on the set of CRPs already stored in the Key Management module challenge-response database as of test DSOSMC:G1:F1:T1 2. The two NORM devices attempt to validate themselves using false response strings; 3. The two NORM devices attempt to validate themselves using correct response strings; 4. Repeat the above for at least 1000 times
Pass criteria	The DSOSMC KMM is able to correctly validate the two NORM devices.
Suspension criteria	N/A

3.1.3.2 Test cases for feature DSNM:G1:F2

Table 5: Test case DSNM:G1:F2:T1

Test ID	DSNM:G1:F2:T1		
Test Description	Test whether the DSOSMC can refresh the active PUF challenge of the various NORMs deployed on the field.		
Test location	At the premises of SYN	**Partner**	SYN
Component	DSOSMC, NORM		
Features under test	DSNM:G1:F2		
Product requirement	The authentication configuration of the various metering devices supported should be periodically and often updated.		
Test environment	An active DSOSMC instance and at least two NORM devices.		
Preparation	N/A		
Dependencies	Test cases DSNM:G1:F1:T1 and DSNM:G1:F1:T2 should have been successfully executed right before this test, considering at least two NORM devices.		
Steps	1. Configure the DSOSMC KMM to update the PUFs active challenge every 1 minute; 2. Record the active challenge of the fake PUFs every minute; 3. Compare the (each minute) recorded active challenges of the fake PUFs with the corresponding challenges sent by the KMM.		
Pass criteria	At any given moment, the active challenge of a PUF should be different than the one in the minute before and should match the one designated by the DSOSMC KMM.		

Suspension criteria	N/A

3.1.3.3 Test cases for feature DSNM:G2:F1

Table 6: Test case DSNM:G2:F1:T1

Test ID	DSNM:G2:F1:T1		
Test Description	Test whether data reported by the NORM devices are encrypted and can be decrypted by the DSOSMC if they have not been tampered with.		
Test location	At the premises of SYN	**Partner**	SYN
Component	DSOSMC, NORM		
Features under test	DSNM:G2:F1		
Product requirement	The DSOSMC should be able to decrypt messages encrypted by the NORM PUF hardware security mechanism.		
Test environment	An active DSOSMC instance and at least two NORM devices.		
Preparation	A predefined message to be encrypted should have been agreed upon.		
Dependencies	All test cases referring to features belonging to DSNM:G1 should have been successfully applied.		
Steps	1. The DSOSMC bootstraps and periodically updates the active challenges of the NORM PUF modules; 2. The NORM devices encrypt the predefined message structure and send it to the DSOSMC; 3. The DSOSMC should be able to decrypt the message;		
Pass criteria	The decrypted message matches the pre-defined one.		
Suspension criteria	N/A		

Table 7: Test case DSNM:G2:F1:T2

Test ID	DSNM:G2:F1:T2		
Test Description	Test whether on-channel data tampering is possible to be detected by the DSOSMC.		
Test location	At the premises of SYN	**Partner**	SYN
Component	DSOSMC, NORM		
Features under test	DSNM:G2:F1		
Product requirement	The DSOSMC should be able to detect if the messages sent by the NORM devices have been tampered with on-channel (detect man-in-the-middle attacks)		
Test environment	An active DSOSMC instance and at least two NORM devices.		
Preparation	A predefined message to be encrypted should have been agreed upon. Also, a service emulating a threat agent listening to the channel (e.g. having broken the VPN connection between the NORM and the DSOSMC) should be available.		

Dependencies	All test cases referring to features belonging to DSNM:G1 should have been successfully applied.
Steps	1. The DSOSMC bootstraps and periodically updates the active challenges of the NORM PUF modules; 2. The NORM devices encrypt the predefined message structure and feeds a third-party service emulating the threat agent; 3. The threat agent emulating service alters the message, changing either the NORM ID, or the encrypted message string, or the timestamp of the encryption reported; 4. The threat agent emulating service forwards the altered message to the DSOSMC for decryption; 5. The DSOSMC should be able to detect the message manipulation and raise an alarm;
Pass criteria	The DSOSMC identifies the decryption failure indicating data manipulation.
Suspension criteria	N/A

3.1.3.4 Test cases for feature DSNM:G2:F2

Table 8: Test case DSNM:G2:F2:T1

Test ID	DSNM:G2:F2:T1		
Test Description	Ensure ability of the NORM to connect through a VPN-encrypted channel to the DSOSMC granted that the credentials and installed certificates are valid.		
Test location	In the premises of REC	**Partner**	REC
Component	DSOSMC, NORM		
Features under test	DSNM:G2:F2		
Product requirement	N/A		
Test environment	An active DSOSMC instance and at least two NORM devices, all configured to connect to the same OpenVPN service.		
Preparation	Configure the OpenVPN client on the NORM and the DSOSMC to use a set of valid credentials and a set of valid certificates.		
Dependencies	N/A		
Steps	1. Power up the NORM and the DSOSMC and set the OpenVPN client to auto-start on boot; 2. Try to connect to the OpenVPN service; 3. Ensure that the connection was successful (a new virtual interface has been created in both NORM and DSOSMC, holding an IP address different than the IP address of the NORM physical networking interface). 4. Ensure that the NORM can communicate with the DSOSCM (e.g. executing DSNM:G1:F2:T1).		
Pass criteria	The NORM and the DSOSMC can communicate properly, their channel being VPN-encrypted.		
Suspension criteria	N/A		

3.1.3.5 Test cases for feature DSNM:G3:F1

Table 9: Test case DSNM:G3:F1:T1

Test ID	DSNM:G3:F1:T1		
Test Description	Smart metrology metering services refer to the fact that NORM can extract the metrology related data from its SMM component, which are available for readout from actors having the right to access this data and send the relevant data to the DSOSMC.		
Test location	In the premises of REC	**Partner**	REC
Component	DSOSMC, NORM		
Features under test	DSNM:G3:F1		
Product requirement	The DSOSMC should be able to receive SMM data from the NORM SMM services.		
Test environment	An active DSOSMC instance and at least one NORM device is assumed, configured to use one metrology meter used in the project.		
Preparation	Ensure that the SMM is correctly attached to the NORM.		
Dependencies	N/A		
Steps	1. Power up the NORM and wait a period of at least one week gathering data and sending them encrypted to the DSOSMC; 2. Enter in the system with administrator rights and download the file with the records; 3. Perform readout of energy indexes from the log file; 4. Compare the indexes from file with the indexes received by DSOSMC.		
Pass criteria	The indexes from two sources are the same for the same timestamp.		
Suspension criteria	N/A		

Table 10: Test case DSNM:G3:F1:T2

Test ID	DSNM:G3:F1:T2		
Test Description	The same as DSNM:G3:F1:T1 but with respect to low-cost PMU measurements		
Test location	In the premises of RWTH	**Partner**	RWTH
Component	DSOSMC, NORM		
Features under test	DSNM:G3:F1		
Product requirement	The DSOSMC should be able to receive PMU data from the NORM low-cost PMU services.		
Test environment	An active DSOSMC instance and at least one NORM device is assumed, configured to use a low-cost PMU.		
Preparation	Ensure that the low-cost PMU has been successfully attached to the NORM device and configure it to send at least 10 messages/second.		
Dependencies	The tests DSNM:G2:F1:T1 and all tests falling under DSNM:G1 should have been successfully executed.		
Steps	1. Power up the NORM and wait for at least one day sending encrypted PMU data to the DSOSMC; 2. Collect the data recorded by the low-cost PMU;		

	3. Compare the data retrieved by the NORM with the ones received by DSOSMC.
Pass criteria	The indexes from two sources are the same for the same timestamp.
Suspension criteria	N/A

Table 11: Test case DSNM:G3:F1:T3

Test ID	DSNM:G3:F1:T3		
Test Description	Test the ability of the DSOSMC to handle multiple data streams coming at high rates.		
Test location	At the premises of REC	**Partner**	REC, RWTH, ENG, SYN
Component	DSOSMC, NORM		
Features under test	DSNM:G3:F1		
Product requirement	The DSOSMC Monitor module should be able to handle a high traffic of incoming messages.		
Test environment	An active DSOSMC instance and at least ten NORM devices are assumed, configured to use a low-cost PMU.		
Preparation	Same as DSNM:G3:F1:T2		
Dependencies	The tests DSNM:G2:F1:T1, DSNM:G3:F1:T2 and all tests falling under DSNM:G1 should have been successfully executed.		
Steps	1. Configure the NORM devices to send at least 10 data packets every second for at least 1 hour; 2. Check that all packets were processed (encrypted, transferred and decrypted at the DSOSMC backend) as expected.		
Pass criteria	All packets should have been successfully retrieved and processed by the Monitor module.		
Suspension criteria	There might be cases where physical resources are simply not enough to accommodate the injected traffic. In this case, scalability of the solution should be tested on IT infrastructures of larger capacity else. The correspondence between IT capacity and traffic should be researched and discussed.		

Table 12: Test case DSNM:G3:F1:T4

Test ID	DSNM:G3:F1:T4		
Test Description	Test the ability of DSOSMC to handle data streams containing irrelevant information.		
Test location	At the premises of RWTH	**Partner**	ENG, REC, RWTH, SYN
Component	DSOSMC, NORM		
Features under test	DSNM:G3:F1		
Product requirement	The DSOSMC should only analyse data that are relevant.		
Test environment	An active DSOSMC instance and at least ten NORM devices are assumed.		
Preparation	Same as DSNM:G3:F1:T2 or DSNM:G3:F1:T3, assuming that all NORMs		

	have been configured to send irrelevant data at random times.
Dependencies	N/A
Steps	1. Configure the NORM devices to send irrelevant data at a percentage of 10% of the messages sent. The message emission rate can be at the range of 10 messages per second; 2. Run the service for at least 1 week; 3. Check if all relevant data have been processed and irrelevant data have been discarded.
Pass criteria	All relevant data should have been processed whereas all irrelevant data should have been discarded.
Suspension criteria	N/A

3.1.3.6 Test cases for feature DSNM:G7:F1

Table 13: Test case DSNM:G7:F1:T1

Test ID	DSNM:G7:F1:T1		
Test Description	Check if NORM can perceive changes in its software configuration and accordingly alert the DSOSMC.		
Test location	At the premises of ENG	**Partner**	ENG
Component	DSOSMC, NORM		
Features under test	DSNM:G7:F1		
Product requirement	The DSOSMC should be able to be aware of the software status on the NORM side (either performing remote software attestation or by means being notified about the result of a local software attestation).		
Test environment	An active DSOSMC instance and a NORM device are assumed.		
Preparation	Two files should be a priori available to the NORM, one completely new to the overall NORM software stack and one constituting a slight change to an existing/well known file of the NORM software.		
Dependencies	The tests DSNM:G3:F1:T2 and all tests falling under DSNM:G1 should have been successfully executed		
Steps	1. Perform a software attestation to check that everything is normal on the current NORM configuration; 2. Add a new executable file (script or binary) in the NORM filesystem; 3. Perform software attestation and let the DSOSMC know about the result; 4. Remove the file and replace another file with an alteration; 5. Perform software attestation and let the DSOSMC know about the result; 6. Replace the altered file with the original; 7. Perform software attestation and let the DSOSMC know about the result.		
Pass criteria	Steps 3 and 5 should indicate that the filesystem has changed. Step 7 should report that the NORM condition is normal.		
Suspension criteria	N/A		

Table 14: Test case DSNM:G7:F1:T2

Test ID	DSNM:G7:F1:T2		
Test Description	Check that the NORM is able to identify changes in its overall integrated configuration and accordingly alert the DSOSMC.		
Test location	At the premises of ENG	**Partner**	ENG, REC, RWTH, SYN
Component	DSOSMC, NORM		
Features under test	DSNM:G7:F1		
Product requirement	The DSOSMC should be able to be aware of the hardware status on the NORM side (either performing remote hardware attestation or by means being notified about the result of a local hardware attestation).		
Test environment	An active DSOSMC instance and a NORM device are assumed.		
Preparation	N/A		
Dependencies	The tests DSNM:G3:F1:T2 and all tests falling under DSNM:G1 should have been successfully executed		
Steps	1. Verify the validity of the NORM/SMM/PUF configuration; 2. Alter the configuration by replacing one of the above elements; 3. Verify that the change is detected and appropriately reported to the DSOSMC; 4. Repeat steps 2-3 until all possible alteration combinations have been tested.		
Pass criteria	The change is always detected and the DSOSMC is aware of the change.		
Suspension criteria	N/A		

Table 15: Test case DSNM:G7:F1:T3

Test ID	DSNM:G7:F1:T3		
Test Description	The NORM should be protected by an antivirus mechanism and the DSOSMC should be aware of its status		
Test location	At the premises of SYN	**Partner**	ENG, SYN, REC
Component	DSOSMC, NORM		
Features under test	DSNM:G7:F1		
Product requirement	NORM should be protected by an antivirus software without affecting real-time actions and the DSOSMC should be aware of threats detected.		
Test environment	An active DSOSMC instance and a NORM device are assumed.		
Preparation	N/A		
Dependencies	The tests DSNM:G3:F1:T2 and all tests falling under DSNM:G1 should have been successfully executed.		
Steps	1. Run an antivirus scan; 2. Check if the virus has been detected and the DSOSMC has been notified.		

Pass criteria	The virus should have been detected and removed (quarantined) and the DSOSMC informed.
Suspension criteria	The NORM does not have enough resources to run the antivirus software. In this case, other options may be analysed, such as external analysis by a trusted party.

Table 16: Test case DSNM:G7:F1:T4

Test ID	DSNM:G7:F1:T4		
Test Description	The NORM should be protected by a firewall and the DSOSMC should be aware of its state.		
Test location	At the premises of SYN	**Partner**	ENG, SYN, REC
Component	NORM		
Features under test	DSNM:G7:F1:T4		
Product requirement	All NORM traffic should be protected by a firewall software and DSOSMC should be aware of the status of the NORMs firewall.		
Test environment	An active DSOSMC instance and a NORM device are assumed.		
Preparation	N/A		
Dependencies	The tests DSNM:G3:F1:T2 and all tests falling under DSNM:G1 should have been successfully executed		
Steps	1. Retrieve from the DSOSMC the list of ports that should be open; 2. Scan all ports of the NORM and send a report to the DSOSMC if a port that does not belong to the list of a-priori known ones is open.		
Pass criteria	All ports should be closed except for the a-priori known ones; in any other case, an alert is sent to the DSOSMC.		
Suspension criteria	N/A		

Table 17: Test case DSNM:G7:F1:T5

Test ID	DSNM:G7:F1:T5		
Test Description	Ensure that the DSOSMC is able to retrieve the logs of the security components of the NORM		
Test location	In the premises of SYN	**Partner**	SYN, ENG
Component	DSOSMC, NORM		
Features under test	DSNM:G7:F1		
Product requirement	The DSOSMC should be able to retrieve security logs from the NORM.		
Test environment	An active DSOSMC instance and a NORM device are assumed.		
Preparation	N/A		
Dependencies	The tests DSNM:G3:F1:T2 and all tests falling under DSNM:G1 should have been successfully executed.		
Steps	1. Select a NORM from the DSOSMC dashboard and ask for their logs;		

	2. The logs should be properly retrieved.
Pass criteria	The NORM logs should be available to the DSOSMC.
Suspension criteria	N/A

3.1.3.7 Test cases for feature DSNM:G10:F1

Table 18: Test case DSNM:G10:F1:T1

Test ID	DSNM:G10:F1:T1		
Test Description	Disconnection of NORM devices with compromised SMM or low-cost PMU[2]		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, ISMB
Component	DSOSMC, NORM		
Features under test	DSNM:G10:F1		
Product requirement	The DSOSMC should be able to deduce that a certain set of NORMs has been compromised (SMM and/or low-cost PMU manipulation) and temporarily disconnect them.		
Test environment	An active DSOSMC instance and at least two NORM devices are assumed, out of which, one is “compromised”, namely set to send erroneous measurements.		
Preparation	The DSOSMC demand and production Analytics and Monitor modules are trained and configured to provide reliable results. The “compromised” NORM has reported enough measurements so that the Analytics module has been properly trained to detect the abnormal values.		
Dependencies	All DSNM:G1-DSNM:G7 test cases should have been successfully executed.		
Steps	1. Verify that DSOSMC automatically obtains encrypted real-time measures from NORM; 2. Verify that only relevant data are handled, the irrelevant ones being ignored; 3. Verify that the reported data are not altered and the decryption process is successfully performed; 4. Verify that analytic is performed on the data and the compromised NORMs are detected; 5. The DSOSMC should identify a certain set of countermeasures, the first of whose should be to disconnect the meter from the grid.		
Pass criteria	The “compromised” NORM gets disconnected from the grid.		
Suspension criteria	The DSOSMC Analytics module does not recognise the “compromised” NORM due to improper or inadequate training. In this case, allow the “compromised” NORM to send data without any alteration for enough time, then execute the test again.		

3.1.3.8 Test cases for feature DSNM:G10:F2

Table 19: Test case DSNM:G10:F2:T1

Test ID	DSNM:G10:F2:T1

[2] When allowed by national law

Test Description	Ensure that the DSOSMC is aware of the software security status of the NORM and can appropriately act in case of virus/malware/rootkit detection		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, RWTH
Component	NORM, DSOSMC		
Features under test	DSNM:G10:F2		
Product requirement	The DSOSMC should be aware of the security state of the NORMs in terms of antivirus, anti-rootkit and anti-malware		
Test environment	An active DSOSMC instance and one NORM device are assumed.		
Preparation	Three files are assumed to be available, acting as i) virus, ii) malware, iii) rootkit. These files should be successively placed into the NORM device.		
Dependencies	All DSNM:G1-DSNM:G7 test cases should have been successfully executed.		
Steps	1. Instruct the NORM to perform a security scan; 2. Notify the DSOSMC about the scan outcome; 3. Place the file containing the virus in the NORM filesystem; 4. Instruct the NORM to perform a security scan; 5. Notify the DSOSMC about the scan outcome; 6. After one hour, place the file containing the malware in the NORM filesystem; 7. Repeat steps 4, 5 8. After one hour, place the file containing the rootkit in the NORM filesystem; 9. Repeat steps 4, 5		
Pass criteria	Step 1 should result in no threat detection, in contrast to step 4, which should always result in detecting the infected files. At all times, the DSOSMC should be informed and the countermeasures taken should be: 1. Instruction to quarantine the infected files if not already quarantined; 2. Instruction to periodically (short-ranged and frequently) run the security inspection; 3. Perform software attestation of the node; 4. If the remote attestation fails, the DSOSMC should request a software re-flash on the NORM (be this intervention physical, namely by sending a security crew on-site, or cyber, namely by remote software flashing).		
Suspension criteria	The infected files are not detected by the security software. In this case, alternatives as to this specific software should be investigated.		

3.1.3.9 Test cases for feature DSNM:G10:F3

Table 20: Test case DSNM:G10:F3:T1

Test ID	DSNM:G10:F3:T1		
Test Description	The DSOSMC should be aware of software attestation failures and be able to mitigate them.		
Test location	At the premises of ENG	**Partner**	ENG, SYN, RWTH, REC
Component	DSOSMC, NORM		
Features under test	DSNM:G10:F3		

Product requirement	SUCCESS should be able to verify the authenticity of the software operating in the NORM devices and act either to fix the issue or to notify the DSO security staff to fix it.
Test environment	An active DSOSMC instance and one NORM device are assumed.
Preparation	At least one SUCCESS source or binary file should be available after being slightly or heavily modified.
Dependencies	All DSNM:G1-DSNM:G7 test cases should have been successfully executed.
Steps	1. The DSOSMC instructs the NORM to perform a software attestation; 2. The NORM informs the DSOSMC of the result of the software attestation (performed by the local security agent); 3. Place the modified file in the NORM filesystem replacing the original one; 4. Repeat steps 1-2 5. The DSOSMC notifies the DSO security staff about the event through the Dashboard; 6. The DSOSMC tries to mitigate the issue; a. The DSOSMC tries to flash a new version of the NORM device software; b. The DSOSMC informs the DSO security staff through the Dashboard that a maintenance unit should be sent to fix the issue.
Pass criteria	Step 2 should result in a report stating that everything is normal. Step 4 should result in a report stating that the software attestation failed. Step 6 should be completed, either using option a or option b.
Suspension criteria	N/A

3.1.3.10 Test cases for feature DSNM:G10:F4

Table 21: Test case DSNM:G10:F4:T1

Test ID	DSNM:G10:F4:T1		
Test Description	The DSOSMC should be aware of hardware attestation failures and be able to mitigate them.		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, RWTH
Component	DSOSMC, NORM		
Features under test	DSNM:G10:F4		
Product requirement	SUCCESS should be able to verify the validity of the hardware configuration of the NORM devices and notify the DSO security staff to fix possible misconfigurations.		
Test environment	An active DSOSMC instance and one NORM device are assumed, the NORM being equipped with PUF and one of SMM or low-cost PMU.		
Preparation	If the NORM is equipped with a low-cost PMU, another low-cost PMU should be available. If the NORM is equipped with a SMM, another SMM should be available.		
Dependencies	All DSNM:G1-DSNM:G7 test cases should have been successfully executed.		
Steps	1. The DSOSMC instructs the NORM to perform a hardware attestation; 2. The NORM informs the DSOSMC over the result of the hardware		

	attestation (performed by the local security agent); 3. Replace the metering (SMM/low-cost PMU) equipment of the NORM with the replacement, or simply remove it. 4. Repeat steps 1-2 5. The DSOSMC notifies the DSO security staff about the event through the Dashboard; 6. The DSOSMC should inform the DSO security staff through the Dashboard that a maintenance unit should be sent to fix the issue;
Pass criteria	Step 2 should result in a report stating that everything is normal. Step 4 should result in a report stating that the software attestation failed. Step 6 should be completed.
Suspension criteria	N/A

3.1.3.11 Test cases for feature DSNM:G10:F5

Table 22: Test case DSNM:G10:F5:T1

Test ID	DSNM:G10:F5:T1		
Test Description	Ensure that the DSOSMC is aware of the firewall status of the NORM and can appropriately act in case of firewall misconfiguration detection.		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, RWTH
Component	DSOSMC, NORM		
Features under test	DSNM:G10:F5		
Product requirement	The DSOSMC should be aware of the security state of the NORMs in terms of firewall configuration.		
Test environment	An active DSOSMC instance and one NORM device are assumed.		
Preparation	N/A		
Dependencies	All DSNM:G1-DSNM:G7 test cases should have been successfully executed.		
Steps	1. Instruct the DSOSMC to perform a security scan on the particular NORM; 2. Notify the DSOSMC about the firewall scan outcome; 3. Change the firewall configuration of the NORM; 4. Repeat steps 1, 2. 5. The DSOSMC, being aware of the firewall misconfiguration, sends to the NORM a valid configuration; 6. The NORM device applies the new configuration; 7. Instruct the DSOSMC to perform a security scan on the particular NORM.		
Pass criteria	Step 1 should result in no firewall misconfiguration detection, in contrast to step 4, which should always result in detecting the firewall rules change. At all times, the DSOSMC should be informed and the countermeasures taken should be: 5. Send to the NORM a valid configuration; 6. Perform a new firewall scan; 7. Perform a remote attestation (see DSNM:G7:F1 and DSNM:G10:F3) If the remote attestation fails, the DSOSMC should request a software re-flash on the NORM (be this intervention physical, namely by sending a security crew on-site, or cyber, namely by remote software flashing).		

Suspension criteria	N/A

3.1.3.12 Test cases for feature DSNM:G10:F6

Table 23: Test case DSNM:G10:F6:T1

Test ID	DSNM:G10:F6:T1		
Test Description	Test the ability of the DSOSMC to identify unreachable NORM devices and appropriately inform the DSO security staff though the DSOSMC dashboard.		
Test location	At the premises of ENG	**Partner**	ENG, SYN, REC, RWTH
Component	DSOSMC, NORM		
Features under test	DSNM:G10:F6		
Product requirement	SUCCESS should be able to detect situations when a NORM is not reachable and notify the DSO security staff.		
Test environment	An active DSOSMC instance and one NORM device are assumed.		
Preparation	N/A		
Dependencies	All DSNM:G1-DSNM:G7 test cases should have been successfully executed.		
Steps	1. Leave the NORM to operate normally for one hour; 2. Plug the NORM out of power; 3. After 5 minutes, plug it in again; 4. Configure the NORM to not use the internet; 5. After 5 minutes, configure it to use the internet.		
Pass criteria	In both step 2 and step 4, the DSOSMC should inform the DSO security staff through the Dashboard that a maintenance unit should be sent to fix the issue.		
Suspension criteria	N/A		

3.1.3.13 Test cases for feature DSNM:G10:F7

Table 24: Test case DSNM:G10:F7:T1

Test ID	DSNM:G10:F7:T1		
Test Description	Test that the DSOSMC is able to identify situations of repeating NORM authentication errors and appropriately acts to fix the issue.		
Test location	At the premises of SYN	**Partner**	SYN
Component	DSOSMC, NORM		
Features under test	DSNM:G10:F7		
Product requirement	The DSOSMC should identify situations of repeating NORM authentication errors and appropriately act to fix the issue.		
Test environment	An active DSOSMC instance and one NORM device are assumed.		

Preparation	N/A
Dependencies	All DSNM:G1-DSNM:G7 test cases should have been successfully executed.
Steps	1. Let the NORM operate normally for one hour; 2. Change the code that handles the PUF-related processes; 3. Instruct the DSOSMC to ask for a NORM validation; 4. Leave the NORM to operate for one hour 5. The DSOSMC should identify that: a. The validation always fails; b. The decryption processes always fail. 6. The DSOSMC attempts to update the active CRP of the NORM and informs it about it; 7. If this does not fix the problem, the DSOSMC instructs the NORM to perform a software and hardware attestation; 8. If this does not fix the problem, the DSO security staff are informed that a maintenance unit should be sent on-site to fix the issue;
Pass criteria	The remote software attestation should identify the problem. Hence, test procedures of DSNM:G10:F3:T1 are invoked.
Suspension criteria	N/A

3.1.4 Test and certification time schedule

Test	Projectmonths														
	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
DSNM:AM:G1:F1															
DSNM:AM:G1:F2															
DSNM:AM:G2:F1															
DSNM:AM:G2:F2															
DSNM:AM:G3:F1															
DSNM:AM:G7:F1															
DSNM:AM:G10:F1															
DSNM:AM:G10:F2															
DSNM:AM:G10:F3															
DSNM:AM:G10:F4															
DSNM:AM:G10:F5															
DSNM:AM:G10:F6															
DSNM:AM:G10:F7															

4. Conclusion

This document constitutes the basis for ensuring the SUCCESS integration and validation tests that ensure that NORM and DSOSMC are seamlessly co-operating from both a logical and functional perspective, particularly in view of the actual field trials testing performed in the context of WP5. In this sense, the objective of the integration and validation tests is twofold; on the one hand, the tests ensure that the integrated NORM and DSOSMC are operating successfully in a laboratory and limited real environment. This will minimize the problems and issues that may arise during the full deployment of the SUCCESS Security Monitoring solution in WP5. The definition of the tests starts by looking at the SUCCESS Security Monitoring solution certification framework defined as a complete set of technical features representing all the functionalities of the NORM DSOSMC pair. These test scenarios are in fact defined to allow the test of all the features presented in the use cases.

The approach ensures the verification of system core functionalities in terms of successful operation testing and integrated performance. The results of the integration tests that are here defined will constitute the outcomes of the third version of this deliverable.

5. References

[1] SUCCESS, «Deliverable D3.10: Integration and Validation Plan. Test and certification specifications, V1,» 2017.

[2] SUCCESS, «Deliverable D3.13: Smart Grid Test & Certification Specifications, V1,» 2017.

[3] «Raspberry PI,» [Online]. Available: https://www.raspberrypi.org/.

[4] SUCCESS, «Deliverable D4.2: Solution Architecture and Solution Description, V2,» 2017.

[5] SUCCESS, «Deliverable D3.4: Information Security Management Components and Documentation v1,» 2017.

[6] SUCCESS, «Deliverable D3.5: Information Security Management Components and Documentation, V2,» 2017.

[7] SUCCESS, «Deliverable D4.8: Integration and WP4 Validation Plan - Test and certification specifications, V2,» 2017.

[8] SUCCESS, «Deliverable D4.9: Integration and Validation Plan - Test and certification specifications, V3,» (expected) May 2018.

[9] SUCCESS, «Deliverable D3.7: Next Generation Smart Meter, V1,» 2017.

[10] SUCCESS, «Deliverable D4.5: Description of available components for SW functions, infrastructure and related documentation, V2,» 2017.

[11] SUCCESS, «Deliverable D1.2: Identification of existing threats V2,» 2017.

[12] D. Tzovaras, A. Adamopoulou, G. Fiorentino, D. Ioannidis, J. Jimeno, D. Kaimaras, C. Malavazos, P. Monti, J. Oyarzabal, N. Ruiz, M. Skokan, P. Tooren, T. Tryferidis, K. Tsatsakis e U. Wingstedt, «D1.3: INERTIA Framework Architecture including functional elements and technical specifications,» INERTIA project deliverable, September 2013.

[13] “LinkSmart software,” [Online]. Available: http://sourceforge.net/projects/linksmart/. [Accessed 05 2014].

[14] N. Ruiz, G. Fiorentino, P. Kostelnik, M. Lipera, J. M. Oyarzabal, P. Van Tooren, T. Tryferidis e K. Tsatsakis, «INERTIA project deliverable D2.4.1: INERTIA Multi-Dimensional Flexibility Models,» 2013.

[15] Almende, “EVE,” [Online]. Available: http://eve.almende.com/.

[16] ENTSOE, “The Harmonized Electricity Market Role Model,” European Network of Transmission System Operators for Electricity, 2011.

[17] J. Jimeno, E. Karfopoulos, D.-E. Archer e P. Van Tooren, «D4.2: Grid Coordination and DR Activation Based on Multi Agents Framework Modules,» INERTIA project deliverable, 2014.

[18] D. Tzovaras, C. Korkas, S. Zikos, A. Tryferidis and J. Jimeno, “D5.1.1: INERTIA Grid-Building-DER integrated prototype,” INERTIA Deliverable, 2014.

[19] D. Tzovaras, C. Korkas, S. Zikos, A. Tryferidis, J. Zabala and J. Jimeno, “D5.3.1: INERTIA prototype Lab Installation including Validation, Parameterization and Testing,” INERTIA Deliverable, 2014.

6. List of Abbreviations

AAA	Authentication authorization accounting
AMI	Advanced Metering Infrastructure
AMR	Automatic Meter Reading
CAPEX	Capital Expenditure
CRP	Challenge Response Pair (referring to PUF-enabled NORM devices)
DSNM	DSOSMC ↔ NORM (integrated system)
DSO	Distribution System Operator
DSOSMC	Distribution System Operator Security Monitoring Centre
EDM	Event Driven Meter
E-SMIS	Pan-European Security Monitoring Information System
GPS	Global Positioning System
KMM	Key Management Module (DSOSMC context)
KPI	Key Performance Indicator
NaN	Neighbourhood Area Network
NORM	Next Generation Open Real Time Smart Meter
OS	Operating System
PMC	PTP Management Client
PMU	Phasor Measurement Unit
PPS	Pulse Per Second
PTP	Precise Time Protocol
PUF	Physical Unclonable Function
ROCOF	Rate of Change Of Frequency
SCADA	Supervisory Control And Data Acquisition
SGAM	Smart Grid Architecture Model
SMG	Smart Meter Gateway
SMM	Smart Metrology Meter
SSH	Secure Shell
SUCCESS	Securing Critical Energy Infrastructures
TVE	Total Vector Error
VM	Virtual Machine
VPN	Virtual Private Network
WP	Work Package

Annex A. Test cases reference

#	Test case ID	Component	Short Description	§	Page
1	DSNM:G1:F1:T1	DSOSMC, NORM	Test that the DSOSMC can bootstrap a PUF-enabled NORM, by registering sets of CRP	3.1.3.1	15
2	DSNM:G1:F1:T2	DSOSMC, NORM	Test that the DSOSMC KMM can identify a PUF-enabled NORM device	3.1.3.1	15
3	DSNM:G1:F2:T1	DSOSMC, NORM	Test whether the DSOSMC can refresh the active PUF challenge of the various NORMs deployed on the field.	3.1.3.2	16
4	DSNM:G2:F1:T1	DSOSMC, NORM	Test whether data reported by the NORM devices are encrypted and can be decrypted by the DSOSMC if they have not been tampered.	3.1.3.3	17
5	DSNM:G2:F1:T2	DSOSMC, NORM	Test whether on-channel data tampering is possible to be detected by the DSOSMC.	3.1.3.3	17
6	DSNM:G2:F2:T1	DSOSMC, NORM	Ensure ability of the NORM to connect through a VPN-encrypted channel to the DSOSMC granted that the credentials and installed certificates are valid.	3.1.3.4	18
7	DSNM:G3:F1:T1	DSOSMC, NORM	Test that the SMM measurements are correctly fed to the DSOSMC	3.1.3.5	19
8	DSNM:G3:F1:T2	DSOSMC, NORM	Test that the low-cost PMU measurements are correctly fed to the DSOSMC	3.1.3.5	19
9	DSNM:G3:F1:T3	DSOSMC, NORM	Test the ability of the DSOSMC to handle multiple data streams coming at high rates.	3.1.3.5	20
10	DSNM:G3:F1:T4	DSOSMC, NORM	Test the ability of DSOSMC to handle data streams containing irrelevant information.	3.1.3.5	20
11	DSNM:G7:F1:T1	DSOSMC, NORM	Check if NORM can perceive changes in its software configuration and accordingly alert the DSOSMC.	3.1.3.6	21

12	DSNM:G7:F1:T2	DSOSMC, NORM	Check that the NORM is able to identify changes in its overall integrated configuration and accordingly alert the DSOSMC.	3.1.3.6	22
13	DSNM:G7:F1:T3	DSOSMC, NORM	The NORM should be protected by an antivirus mechanism and the DSOSMC should be aware of its status	3.1.3.6	22
14	DSNM:G7:F1:T4	DSOSMC, NORM	The NORM should be protected by a firewall and the DSOSMC should be aware of its state.	3.1.3.6	23
15	DSNM:G7:F1:T5	DSOSMC, NORM	Ensure that the DSOSMC is able to retrieve the logs of the security components of the NORM	3.1.3.6	23
16	DSNM:G10:F1:T1	DSOSMC, NORM	Disconnection of NORM devices with compromised SMM or low-cost PMU (disconnection possible when allowed by national law)	3.1.3.7	24
17	DSNM:G10:F2:T1	DSOSMC, NORM	The DSOSMC is aware of the software security status of the NORM and can appropriately act in case of virus/malware/rootkit detection	3.1.3.8	24
18	DSNM:G10:F3:T1	DSOSMC, NORM	The DSOSMC should be aware of NORM software attestation failures and be able to mitigate them.	3.1.3.9	25
19	DSNM:G10:F4:T1	DSOSMC, NORM	The DSOSMC should be aware of NORM hardware attestation failures and be able to notify the DSO security monitoring stuff	3.1.3.10	26
20	DSNM:G10:F5:T1	DSOSMC, NORM	The DSOSMC should be aware of the firewall status of the NORM and can act in case of firewall misconfiguration detection	3.1.3.11	27
21	DSNM:G10:F6:T1	DSOSMC, NORM	The DSOSMC should be able to identify and inform the DSO over unreachable NORM devices	3.1.3.12	28
22	DSNM:G10:F7:T1	DSOSMC, NORM	Test that the DSOSMC is able to identify situations of repeating NORM authentication	3.1.3.13	28

			errors and appropriately acts to fix the issue.		