success

D4.4 v1.0

Description of Available Components for SW Functions, Infrastructure and Related Documentation, V1

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:	**31.01.2017**
Contributors:	RWTH, EDD, P3E, P3C, LMF, ENG
Workpackage:	WP4 – Securing Smart Infrastructure
Estimated person months:	10
Security:	PU
Nature:	R
Version:	1.0
Total number of pages:	48

Abstract:

This document describes the success Security Monitoring Solution which is the instantiation of the success architecture in the infrastructure developed by the success project itself. The functionality of the components in the success infrastructure and the interfaces between them are described. In addition, a set of security countermeasures to threats is defined and the way that the countermeasures are executed by means of the components in the success infrastructure is described. Hence, this deliverable maps the success countermeasures onto the components' functionality and the interfaces between the components.

Keyword list:

Security, communication, Utility, Architecture, Threat, Countermeasure

Executive Summary

This document describes the success Security Monitoring Solution which is the instantiation of the success security architecture. success is developing a Pan-European Security Monitoring Centre (ESMC), consisting 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. Both, E-SMIS and DE-SMIS, work together to detect patterns related to cyber-attacks and to alert DSOs or TSOs about attacks.

success is also developing the DSO Security Monitoring Centre which, based on data gathered from the distribution grid, identifies attacks and applies countermeasures. In the success infrastructure, data is provided by the NORM (the Smart Meter Gateway being developed by success) to the DSO Security Monitoring Centre, which analyses the data to detect cyber-attacks and apply countermeasures. The DSO Security Monitoring Centre provides its local DE-SMIS instance with information on applied countermeasures and grid status. DE-SMIS processes this information by interacting with E-SMIS and by resorting to further data sources.

Countermeasures are also implemented through the Breakout Gateway, which is a new mobile communications node being developed in success, which allows mobile core network functionality to be implemented on the edge of the network (e.g. in a cloud system located on the eNodeB). The Breakout Gateway supports Data Centric Security (checking of packet integrity without decoding the packets) and Generic Bootstrap Architecture (authentication performed locally on the BR-GW).

success is developing a resilience solution for the power and communication grids based on a separation of applications from their data and the execution of the functionality related to the application and data parts on separate Virtual Machines in a cloud infrastructure. In case of cyber-attack, a countermeasure to move the application or data functionality to another Virtual Machine. can be applied.

This deliverable contains a list of the countermeasures that can be applied to cyber-attacks on the success infrastructure, together with a mapping onto the components and functions that implement the countermeasures.

This first version of this deliverable documents the current status of the design of the success Security Monitoring Solution. The later versions will provide more details of the components and their interfaces.

Authors

Partner	Name	e-mail
RWTH Aachen University (RWTH)		
	Padraic McKeever	pmckeever@eonerc.rwth-aachen.de
	Gianluca Lipari	glipari@eonerc.rwth-aachen.de
OY L M ERICSSON AB (LMF)		
	Patrik Salmela	patrik.salmela@ericsson.com
ERICSSON GmbH (EDD)		
	Dhruvin Patel	dhruvin.patel@ericsson.com
	Zain Mehdi	zain.mehdi@ericsson.com
	Frank Sell	frank.sell@ericsson.com
P3 ENERGY & STORAGE GmbH (P3E)		
	Manuel Allhoff	Manuel.Allhoff@p3-group.com
Engineering – Ingegneria Informatica SPA (ENG)		
	Antonello Corsi	antonello.corsi@eng.it
	Giampaolo Fiorentino	giampaolo.fiorentino@eng.it
P3 Communications GmbH (P3C)		
	Panagiotis Paschalidis	Panagiotis.Paschalidis@p3-group.com
Centrul Roman al Energiei (CRE)		
	Mihai Paun	mihai.paun@crenerg.org
	Mihai Sanduleac	mihai.sanduleac@crenerg.org

Table of Contents

1. Introduction

The success architecture has been described in the deliverable D4.1 [1] from the Electricity Distribution and Transmission Utilities, Communications and Security viewpoints. This architecture is not specific to the success project but may be instantiated in different particular systems. The success architecture covers security management and monitoring by means of enhanced mobile communications technologies applied to smart distribution grids.

This document describes the success Security Monitoring Solution which is the instantiation of the success architecture in the infrastructure developed by the success project itself. The functionality of the components in the success infrastructure and the interfaces between them are described. In addition, a set of security countermeasures to threats is defined and the way that the countermeasures are executed by means of the components in the success infrastructure is described. Hence, this deliverable maps the success countermeasures onto the components' functionality and the interfaces between the components.

This document is an output of Task 4.2 of success, which is concerned with architecture definition. This is the first, preliminary, version of the document. Two further updated versions will be produced in the course of the project.

Addressing cybersecurity is critical to enhancing the security and reliability of both the transmission and distribution electricity grids. Ensuring a resilient HV electricity grid is particularly important since it is one of the most complex and critical infrastructure that other sectors depend upon to deliver essential services. Over the past two decades, the roles of electricity sector stakeholders have shifted: generation, transmission, distribution and supply functions have been separated into distinct markets; customers have become generators using distributed generation technologies; and vendors have assumed new responsibilities to provide advanced technologies and improve security. These changes have created new responsibilities for all stakeholders in ensuring the continued security and resilience of the electricity Transmission and Distribution grids.

Cybersecurity is a serious and ongoing challenge for the energy/electricity sector. Cyber threats to electricity delivery systems can impact national security, public safety, and the national economy. Because the private sector owns and operates most of the energy sector's critical assets and infrastructure, and governments are responsible for national security, securing energy delivery systems against cyber threats is a shared responsibility of both the public and private sectors. A common vision and a framework for achieving that vision are needed to guide the public-private partnerships that will secure electricity delivery systems.

There are very many recent cyber security attacks events in the electricity grid. A list of the most relevant and recent ones registered in the electricity HV transmission and in the electricity distribution grids is given in Appendix A.

The document is structured as follows:

Ch. 2 describes firstly in Ch. 2.1 the success infrastructure in terms of Application, Communications and Utility (Electricity Distribution Grid) layers. success concentrates on the Distribution level of the Electrical Grid, where the NORM Smart Meter Gateway is introduced. Details of the NORM are outside the scope of this document and will be provided in success D3.7 in April 2017 (M12 of the project).

The success Security Monitoring Solution is described in Ch. 2.2: this Solution shows how the components of the success infrastructure work together to detect security threats to the Electricity Distribution Grid's management and communication systems and execute countermeasures which mitigate these threats.

success is concentrating on how mobile 5G communications can be applied to Utility communications to provide enhanced security functionality. The communication features used

by success are described in Ch. 2.3. The approach of success to achieving security of its components and communications is outlined in Ch. 2.4.

The DSO Security Monitoring Centre (DSOSMC) and the Pan-European Security Monitoring Centre (ESMC) are described in Chs. 2.5 and 2.6. The DSOSMC monitors and generates countermeasures for particular local electricity distribution grids. ESMC is intended to monitor a large area and to alert DSOs or TSOs in case of security threats. ESMC comprises a central instance (E-SMIS) and several decentralized instances (DE-SMIS), which interwork with the DSOSMCs.

Task 2.3 of success ("Resilience by Design") is studying how virtualisation of functionality in the electricity transmission and distribution grids and in the communications network can enhance the resilience of both grids to security threats. This "double virtualisation", outlined in Ch. 2.8, allows the virtual machine (VM) hosting the functionality to be changed as a countermeasure to certain attacks.

The DSOSMC and ESMC will be tested in the success field trials, as will the NORM. Double Virtualisation is a research topic in success; it will not be tested in the field trials of WP5, therefore, but a laboratory demonstration of Double Virtualisation will be performed as part of WP2.

The interfaces between the components of the success Security Monitoring Solution are outlined in Ch. 2.7.

The rest of the document comprises a list of Threats and applicable Countermeasures (Ch. 3) and a set of chapters, one per Countermeasure, beginning with Ch. 4) which describe the Countermeasure and how it will be implemented by the components of the success Monitoring Solution.

This first version of this deliverable documents the current status of the design of the success Security Monitoring Solution. The later versions will provide more details of the components and their interfaces.

2. Infrastructure Description

2.1 success Infrastructure

The components in the infrastructure developed by the success project are shown in Figure 1, forming an instantiation of the success architecture described in D4.1 [1].

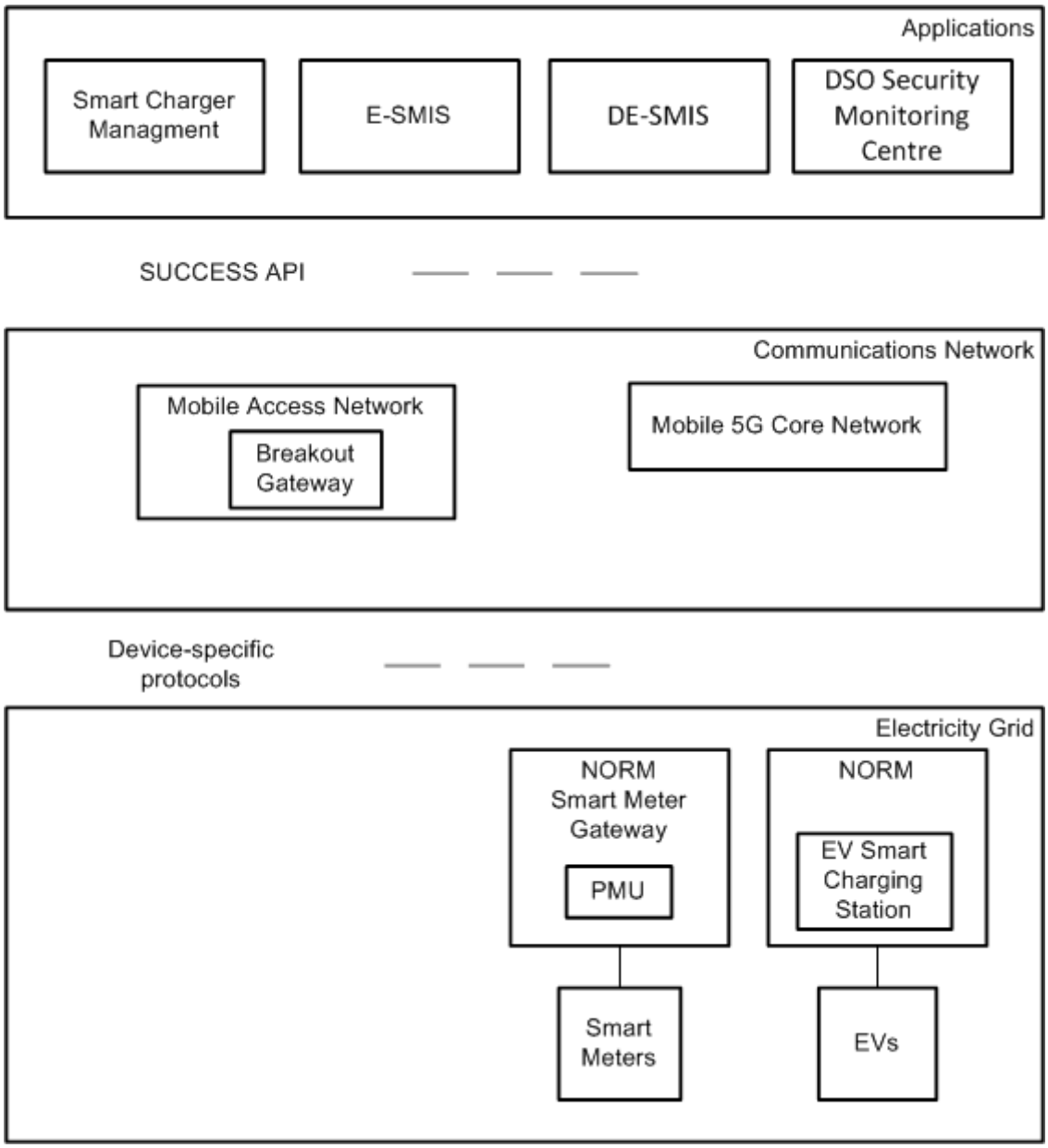

Figure 1: success Infrastructure

The success infrastructure comprises the electricity grid, communications infrastructure and applications.

The success project will perform field trials in Italy, Romania and Ireland, testing the success infrastructure in the real electricity grids in these countries. In addition, simulated grids will be used for tests in laboratory environments. The details of these grids (such as the power generators, transmission and distribution cables, transformers, loads etc.) are not drawn in

Figure 1, which just shows the components which success will introduce into the grids. These are:

- the New-generation Open Real-time Smart Meter (NORM), which is produced by success and will be described in detail in deliverable D3.7, due in April 2017.
- a new Phasor Measurement Unit, which is produced by success and will run as one of the components in the NORM and will be described in detail in D3.7.
- Smart Meters of various types which will be present in the field trials and laboratory (if they are connected to the Smart Meter Gateway of NORM, they are also considered as components of NORM),
- Electric Vehicles (EVs) and corresponding charging stations which will be part of the Irish field trial,

success is focussing on the security capabilities offered by mobile communications, particularly 5G communications. This means success reuses the security features of the 5G mobile network but also extends them with the Breakout Gateway. Please note, however, that 5G mobile communications is just one infrastructural component in the success Security Monitoring Solution described in Ch. 2.2 below and that the success Security Monitoring Solution itself does not require 5G mobile communications but other communications networks, albeit with the consequence that no 5G-Mobile-specific functions will then be available. Indeed, because 5G technologies are still under development and are not yet commercially available, the success trial sites are expected to use communications solutions other than 5G mobile and it is expected that the use of 5G mobile technologies in success will be limited to laboratory tests.

success is developing a new Breakout Gateway (BR-GW) which allows mobile core network functionality and application functionality to be executed in the mobile radio network, reducing communication latency and enabling dedicated security functionality. Additionally, with respect to securing the NORM-DSO Security Monitoring Centre communications and guaranteeing authentication while incurring only a minimal communications overhead, a solution based on using a Physically Unclonable Function (PUF) has been considered. By introducing PUF, success is providing NORMs with hardware security features which inherently guarantee that the NORM's identity cannot be tampered with or faked, as PUFs act as a unique identifier, their uniqueness being bound to their specific hardware construction characteristics, also considering environmental or explicitly-introduced randomness. In contrast to TPM [1], PUFs (particularly the ones relaying on intrinsic randomness) can be added in the NORM infrastructure without requiring any change to the manufacturing/design process of the NORM. Further details on the PUF implementation of success will be provided in deliverable D3.7, due in April 2017.

The components grouped as Applications in Figure 1 perform functions related to managing the underlying electricity grids. Figure 1 shows the Applications being developed in success. In success, security attacks will be detected and countermeasures initiated by DSO Security Monitoring Centres, which gather data from a set of NORMs and searches for specific patterns with machine learning methods.

The components of the success infrastructure work together to implement a holistic security monitoring solution, called the success Security Monitoring Solution and described in Ch.2.2, with a focus on the vulnerabilities introduced by smart devices in electrical distribution grids.

The Irish field trial will host an application to manage the smart charging of the EVs.

The Romanian trial will use NORMs in selected points of the network dealing with distributed energy production and relevant distribution network sections and will use available communication solutions which exist in the country (3G or 4G may be available based on the coverage offered by communication providers in the site).

Security is not shown as a component in Figure 1. This is because security functionality in success is distributed throughout the system components and because success does not have

[1] http://www.trustedcomputinggroup.org/trusted-platform-module-tpm-summary/

any dedicated security hardware systems. The security countermeasures are carried out using the functionality of the components shown in Figure 1.

2.2 success Security Monitoring Solution

The infrastructural components introduced in Chapter 2.1 interwork together in the success Security Monitoring Solution to detect security threats and execute countermeasures. Figure 2 gives a functional overview of the success Security Monitoring Solution, showing the components arranged into functional layers and the interfaces between the components.

The Security Monitoring components are located in two layers:

- the DSO/TSO level (see DSOSMC and DE-SMIS at the centre of Figure 2), and
- the pan-European level (see E-SMIS at the top of Figure 2).

E-SMIS and DE-SMIS form the Pan-European Security Monitoring Centre (described in Ch. 2.6), which consists of a single European-level Security Monitoring and Information System (E-SMIS) and several decentralised E-SMIS instances (called DE-SMIS). The Pan-European Security Monitoring Centre (ESMC) performs data analytics to detect patterns that (D)E-SMIS users (the DSOs or TSOs) can potentially use in a downstream process to trigger countermeasures. Please note, however, that the generation of such countermeasures by DSOs or TSOs is outside the scope of the success project. In the success Security Monitoring Solution,

- any countermeasures that are initiated by a DE-SMIS are communicated to the concerned DSO Security Monitoring Centre(s), and
- any countermeasures that are initiated by E-SMIS are communicated to the concerned DE-SMIS(s), and further communicated to the concerned DSO Security Monitoring Centre(s),
- the DSO Security Monitoring Centre(s) are responsible for executing the countermeasures initiated by (D)E-SMIS in the Communications Network and Electricity Grid.

NORM devices located in the distribution grid measure consumer, prosumer or grid-related data. Selected data produced by NORM, which may be relevant for the security assessment at higher levels, are provided to the DSOSMC by a Security Agent running in NORM through the communications network, where the BR-GW component is introduced by success (and other existing communications components are not shown in Figure 2). The interfaces used by the NORM to gather data are not shown in Figure 2 but can be seen in Figure 1.

The DSOSMC receives data from NORMs directly over Interface 1 or via BR-GW over Interface 2. After analysing the data, the DSOSMC provides the results to a DE-SMIS instance via Interface 3. Both DSOSMC and DE-SMIS instances lie on the DSO/TSO level where they interact in a 1:1 relationship. DE-SMIS instances receive data from

- the DSOSMC (see Interface I3), related to detected threats and initiated countermeasures,
- further internal data sources (see Interface I7),
- other DE-SMIS instances located at other DSO/TSOs (see Interface I4); and
- the E-SMIS instance (see Interface I5).

Hence, DE-SMIS receives data from a wide variety of data sources. In particular, DSOSMC is only one among many of such sources. The rationale is that DE-SMIS uses data mining methods on the data from the different data sources to extract new meaning and information about the status of the system.

The E-SMIS instance receives data from DE-SMIS instances and from external security-related data sources, such as logs, and social media streams (see Interface 6). The E-SMIS and DE-SMIS instances together build the pan-European Security Monitoring Centre (ESMC, see Ch. 2.6 for details).

In the success Security Monitoring Solution, besides the (D)E-SMIS, the DSOSMC and the Breakout gateway can also initiate countermeasures. However, in fact, in the success project, only DSOSMC and BR-GW will initiate countermeasures. The countermeasures are executed through the DSO Security Monitoring Centres, the Breakout Gateways and the Double Virtualisation logic.

The success Security Monitoring Solution's interfaces are described further in Ch. 2.7.

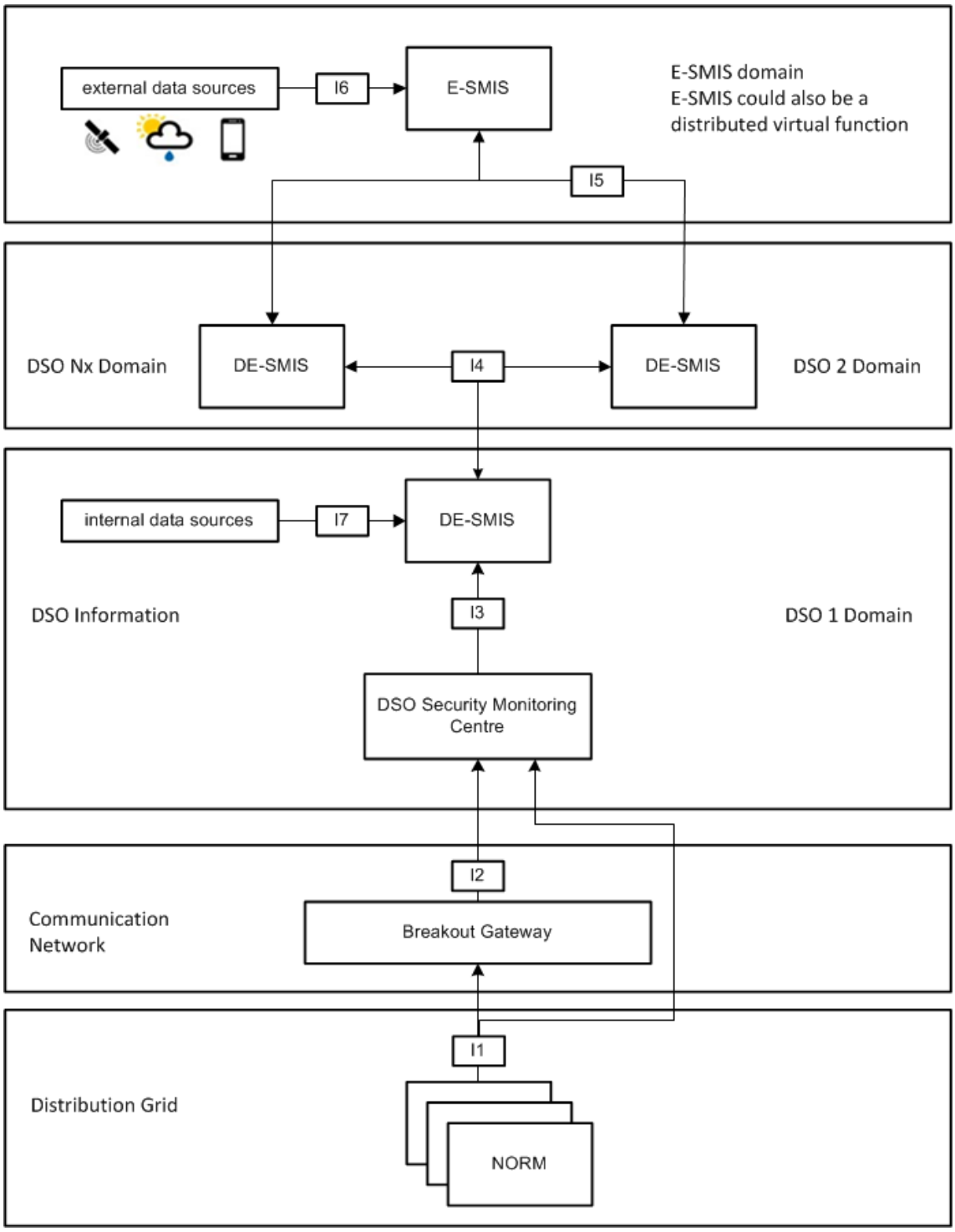

Figure 2: success Security Monitoring Solution. Interfaces between the elements are denoted as I1…I7

It is useful to distinguish between the success Security Monitoring Solution (which contains all the interfaces and components of success) and a particular implementation, for example in a success trial site, which may not contain all the components shown in Figure 2.

2.3 Communication Components

The success communication solution is based on the currently evolving mobile communication infrastructure. This next generation cellular infrastructure aims to fulfil the communication requirements for machine-to-machine (M2M) type communications involving use cases such as smart grid communications. As explained in the D4.1 [1], smart grid communications can be broadly divided into two categories, massive M2M type communication (Advanced Metering Infrastructure, Wide area monitoring) and critical M2M type communication (real time monitoring and grid control, FLISR applications). Enhancements of the current LTE network are being investigated to support both the above use cases. An overview of the LTE network is given in Appendix B.

The 5G communication solution aims to provide seamless connectivity while at the same time ensuring the security of the communication and being able to interwork with any non-3GPP access network (non-cellular network), which might be the communication network in certain smart grid scenarios.

3GPP technology such as Generic Bootstrapping Architecture (GBA) can be utilised to authenticate applications running over 3GPP and non 3GPP network by leveraging trust of SIM card subscription data. Figure 3 shows an overall view of the 3GPP and non 3GPP network domain. A detailed explanation of the Generic Bootstrapping Architecture (GBA) is given later in the current section. Advanced mobile networks such as LTE already have embedded ciphering and integrity protection of the transmitted data over the cellular network.

In success, Data Centric Security is investigated for enabling end to end checking of data integrity against data manipulation and false data injection threats. These threats are considered very crucial for the smart grid applications such as power grid state estimation [7] and voltage control [4] [11].

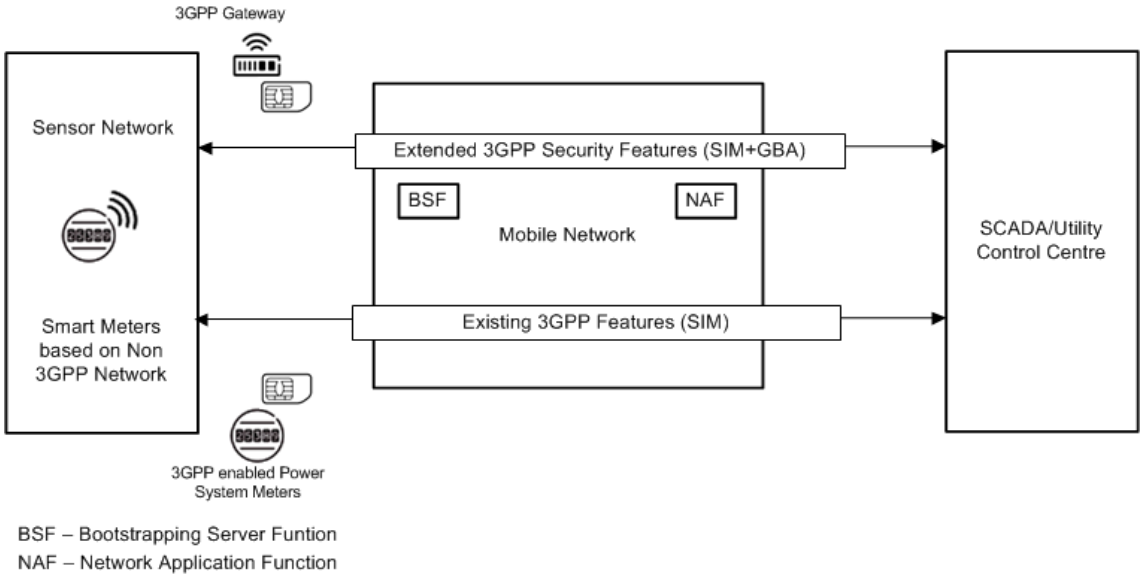

Figure 3: 3GPP domain and extension of 3GPP security features

2.3.1 Break-out Gateway (BR-GW)

Future smart grid use cases are expected to generate huge data streams from the metering infrastructure. These data streams of measurements will flood the network as used currently. Limitations on efficient handling of the massive volumes of data needed to support real time use

cases and to enable real time countermeasure is observed with current communication networks. To enable such use cases, current 5G network technology enablers are being investigated [6]. Specifically, in this project breakout strategies enabling edge processing for real time applications are being developed. They will be hosted in a cloud environment located at the edge of the communications network. Such a breakout gateway can enable distributed data processing and will perform real time countermeasures at the network edge, reducing the impact of local failures and reducing response time.

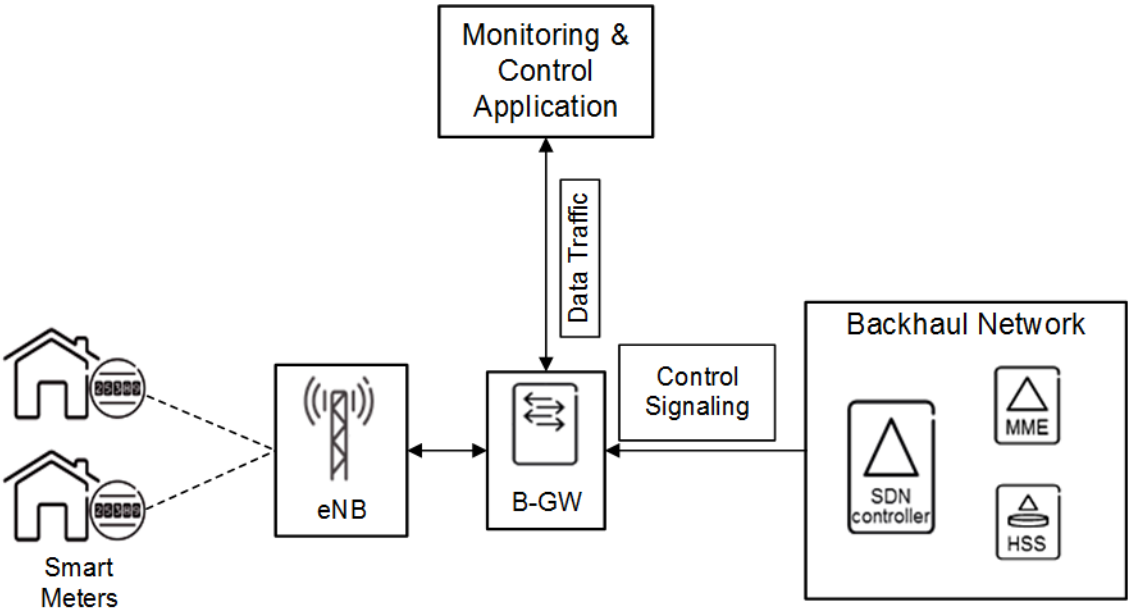

Figure 4: Breakout Gateway

As part of success, the Breakout Gateway is being developed. This local breakout is enabled based on Software Defined Networking (SDN) which will be an integral part of the 5G network architecture [6]. Figure 4 shows the placement of Breakout gateway in the current cellular network. SDN and Network Function Virtualisation (NFV), which are introduced in [2], are prominent technology enablers for 5G. This Breakout gateway will be hosted on hosted on the virtualised environment. A conceptual block diagram of how BR-GW can be realised in Figure 5.

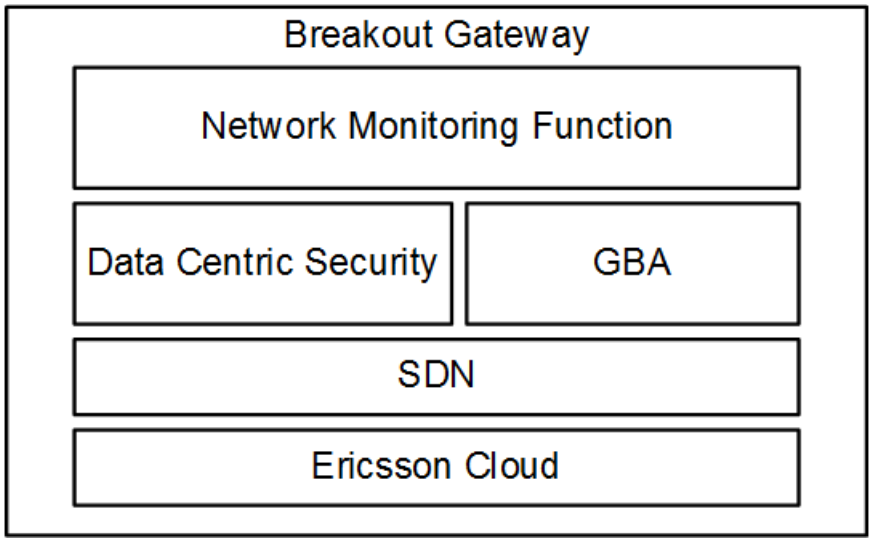

Figure 5: Conceptual diagram of Breakout Gateway

SDN works on the principle of separating the control plane and the data plane. It aims to provide a logically centralised network intelligence and a standardised interface for software development to control network resources and the flow of network traffic. Basic SDN components include the SDN controller, network elements and applications used to control network resources. The SDN controller interacts with applications via standardised Application Programming Interfaces (APIs) and on other side with network elements with standard protocols such as OpenFlow [12]. The applications can implement network services like routing, security and bandwidth management, with different behaviour for traffic in different flows, i.e. from different sources, responding to real-time demand changes in the network. In this project, the Breakout Gateway is based on SDN technology allowing dynamic configuration of the network based on the application requirement.

The impact of the BR-GW on the communication network can be observed from two perspectives, infrastructural impact, and functional impact.

Infrastructural impact: Introducing such a node will reduce the latency and complexity of the core network. It will enable edge power grid monitoring and control applications (decentralised functions). Figure 6 shows the infrastructural impact on the current cellular network. The advantage of introducing the BR-GW is to enable security measures on dedicated power grid traffic while at the same time enabling edge processing for distributed power grid applications.

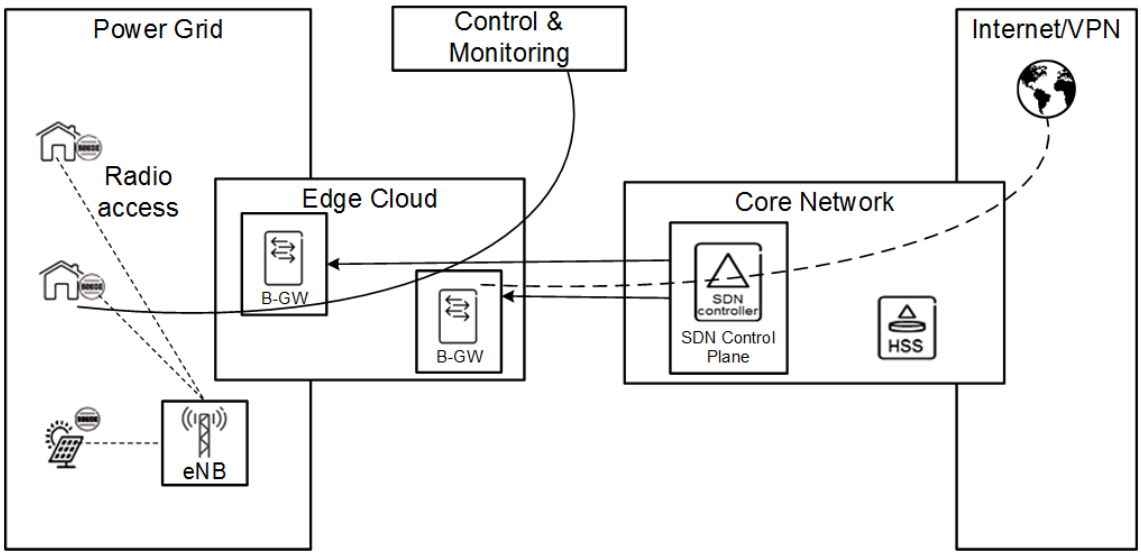

Figure 6: Network architecture based on 5G breakout solution

The **Functional impact of BR-GW** on the communication network can be observed through the functional enhancements it enables, as described below,

- Data Centric Security (DCS):

  DCS enables data integrity check of the end to end information flow in any communication network. Smart meter critical data that are used for power grid state estimation or voltage control [4][7][11] could, if manipulated, disrupt the output of the power grid applications. Such attacks are commonly referred to as False Data Injection attacks (which come under the heading of Incident I7, “Device behaving suspiciously”, in Table 1 of Ch. 3 and in Ch.10). Data integrity of the measurements being communicated over any network should be protected and checked at the entry and exit points.

  DCS focuses on eliminating the security threats caused by data manipulation and authenticates measurement data used by above mentioned power grid applications. It

uses Keyless Signature, i.e. it uses a hash value to detect the manipulation of the data. The idea of the solution is to compute the hash value of the data that is being transmitted using a hashing algorithm such as SHA-256. The system will create a signature from the hash value which is sent, along with the data, to the application centre. The control centre can then verify that the data are correct and has not been tampered with. In this particular solution, the integrity check of the data will be done at BR-GW in a continuous fashion depending upon the application requirements. The integrity checking procedure involves the computation of a hash value from received data; based on this hash value and the signature, the integrity of data is checked.

The DCS solution has a small thin client on smart measurement devices which is connected to data centric security services. The solution can be realised in two implementation options, as shown in Figure 7. One option is that the client will be installed on the smart meters and/or a gateway (data concentrator) that will compute the hash and create the signature, this signature will be sent to the end application server where the data will be verified. The other option is to send the data and hash of the data first to the local BR-GW where a DCS client on the BR-GW will be then responsible for getting the signature from the DCS server and then sending it to the service provider control centre to verify the data. Here the signature itself is a hexadecimal string of hash values, which is different compared to the public key cryptography system.

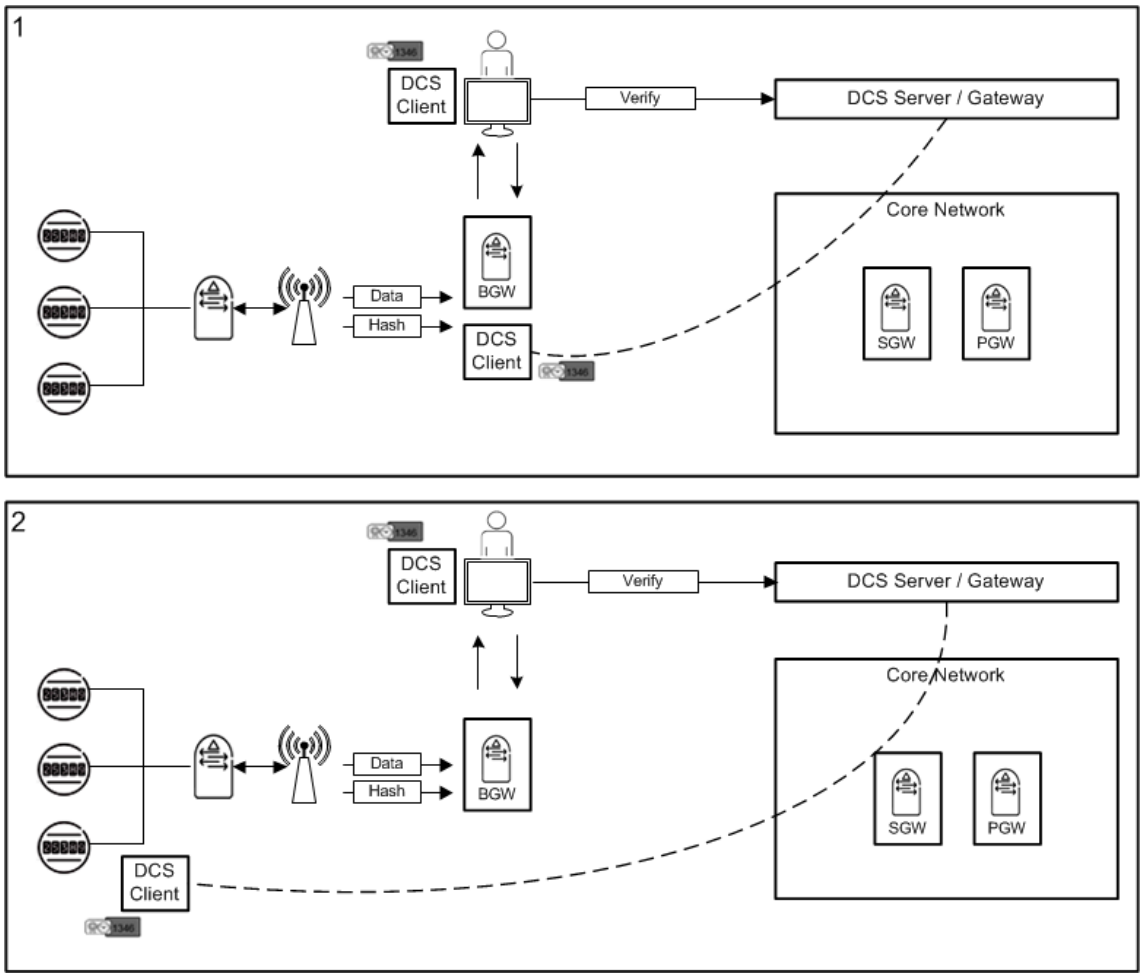

Figure 7: Data Centric Security Options

- Generic Bootstrapping Architecture:

  Generic Bootstrapping Architecture (GBA) is a 3GPP authentication architecture. GBA is standardized in 3GPP standard TS 33.220 [8].

  The reason for using GBA for authentication is to leverage the trust of mobile communication operator to enable authentication of smart grid applications running over 3GPP or non 3GPP network. Compared to state of art solutions such as Public Key Infrastructure and digital certificates, GBA provides a novel solution to authenticate a power grid application running over remote measurement and control devices.

  GBA provides a means to use mobile network subscriber data - which a mobile network operator keeps in its mobile network - to authenticate mobile network users for application services. These other services need not necessarily be under the control of the mobile network operator. In fact, the ability to use mobile network subscriber data to authenticate 3rd party services is a key feature of GBA. Further, GBA supports interoperator authentication.

  GBA can be applied to local breakout services, so that security functions can be provided as well to localised enterprise functions. Figure 8 shows the setup of the GBA in mobile network. Network Application Function (NAF) and Bootstrapping Server Function (BSF) are the two main new components included in GBA.

  In mobile communication networks, HSS is main database containing information used to authenticate User Equipment in the network. BSF sits in front of the HSS and protect the HSS from direct access by 3rd parties and provides necessary information for GBA to enable authentication of application/user.

  NAF is connected to BSF via Zn interface. NAF's main function is to verify the authentication of application messages generated from mobile phones (UEs). NAF acts as message authenticator for any service application. This authentication is done by utilizing subscriber information stored in the HSS via BSF.

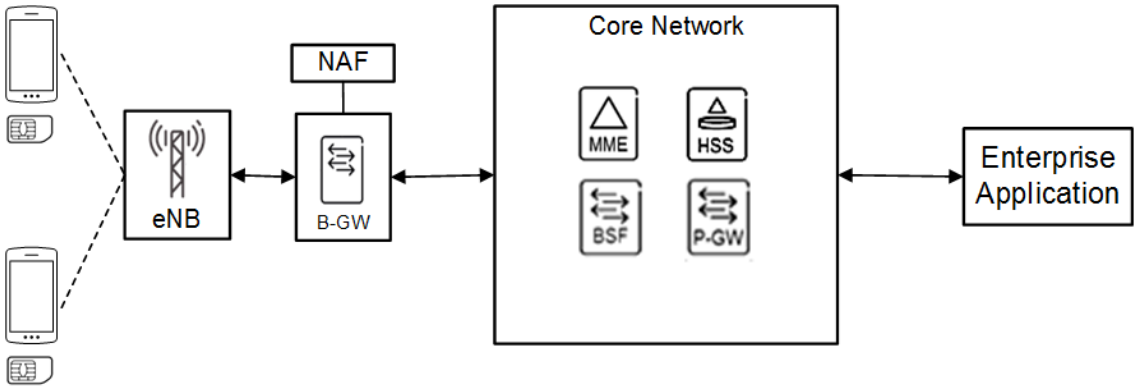

Figure 8: GBA functions applied at Breakout Gateway

  In this BR-GW, NAF functionality can be embedded to authenticate smart grid application generating messages from smart meters connected over 3GPP or non 3GPP networks. Figure 8 shows the realisation of NAF function in BR-GW.

- **Network Monitoring Function (NMF)**: This communication network function enables close investigation of the smart grid related communication traffic. It will enable detection of network threats such as DDoS, IP spoofing, etc. Further details of the solution approach for this will be described in later version of the document.

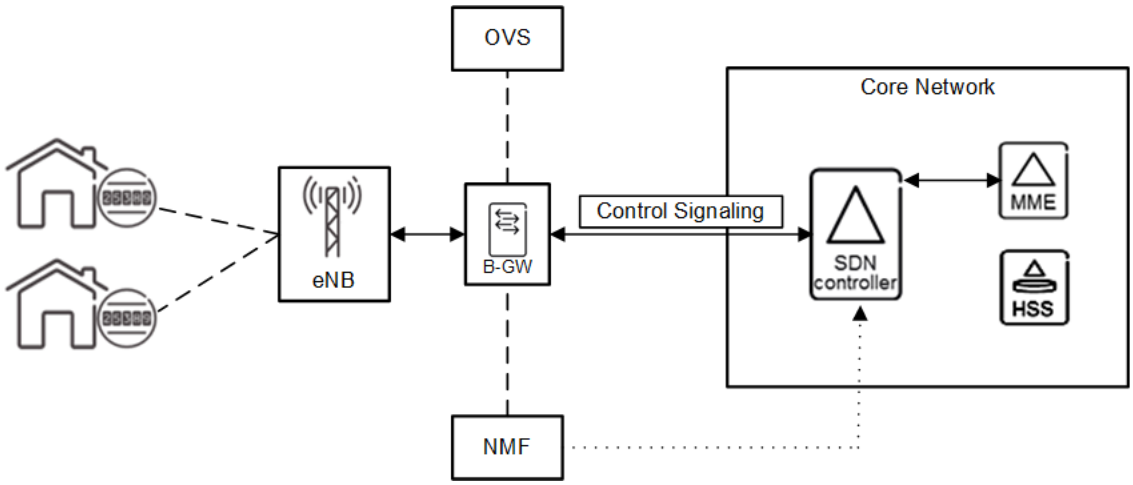

Figure 9: Network Monitoring Function in BR-GW

In Figure 9 above, NMF is part of BR-GW and its main responsibility is to inspect packets to detect anomalies in the packets. NMF monitors packets going through BR-GW and based on the results from its inspection notifies the DSO Security Monitoring Centre (DSOSMC) and can block traffic originating from the particular node. NMF will have small sub-functions for each type of anomaly detection e.g., DDoS, Spoofing, Malware, etc.

Depending on availability of the components, solutions will be tested against the different power grid scenarios. A live LTE network comprising of the above described components will be integrated with state-of-art research facility at RWTH University's ACS lab. BR-GW functionality will be developed and integrated at the RWTH ACS lab with existing LTE network infrastructure. Testing of the functionality will be done with hardware-in-the-loop simulation for a local grid control application. Interface functionality will be realised in the laboratory. Also, it is planned to connect the Irish trial site, consisting of a smart Electrical Vehicle charging system, with the ACS lab setup which includes BR-GW.

2.4 Security Components

All the information communicated between entities in the smart grid is sensitive. The levels of sensitivity range from end-user privacy concerns to business and operation critical information. Integrity and confidentiality protection are the two main types of protection mechanisms mentioned in many architectures. Similar to the information sensitivity, the levels of protection offered by integrity and confidentiality protection vary. Furthermore, security cannot be seen as a separate tool/add-on in individual protocols, components, and architecture descriptions. Instead, it begins with the individual protocol decisions, is embedded into the components of the architecture, and is executed according to scrutinized processes and operating procedures.

Like many critical systems, smart grid communication requires protection against modification. Much of the information can be privacy sensitive and often requires also protection against unauthorized access to the communicated information. The information can either directly or based on data analysis reveal information about a customer and his behaviour. The information also relates to financial transactions, so modification of the information could result in financial loss for either party. Moreover, the security requirements may extend even beyond the communication event, and in some cases create additional security requirements for data storage and handling.

In addition to the information exchanged between the smart meter at the client's premises and the network, the nodes within the power infrastructure also exchange information with high security requirements. This information includes management of the nodes in the network, statistics reporting and network state information.

The basic security for the network includes both the security functions needed for enabling secure communication but also the physical security measures needed for securing the network components against physical threats to the equipment. Physical threats include both malicious attacks with intent to disrupt service by destroying network components as well as other causes of equipment malfunction such as natural phenomena or component malfunction.

2.4.1 Communications Security

The basis for communications security is the device identity, which consists of an identifier and an associated credential. An example of this is a public key certificate as the identifier and the corresponding private key then taking the role of the credential. Also, symmetric key based credentials are possible, where the identifier is a device identity such as the 128-bit universally unique identifier (UUID) and the associated credential is a secret key. In this case, it is important to have a strong enough key, meaning a long enough and random key. The drawback with symmetric approaches is that you can (should) not use the same key towards multiple peers/services as the likelihood of a key being compromised increases and at the same time the effect of it is in theory amplified directly related to the number of entities sharing the same secret key.

However, before the device can use the identity, the identity needs to be provisioned to the device. This is known as security bootstrapping and entails providing the device with all required security configuration; credentials, configuration about which protocols to use and which peers/services to connect to. Furthermore, access control information is configured and installed, software is verified to be up-to-date. In addition to bootstrapping this information to the device, the network also needs to be made aware of the new device that will be installed into the network. This can be done a-priori to device installation and connection to the network or as part of the device installation process. The minimum requirement is that the device identity is provided to at least one authentication server so that the device is able to authenticate itself to peers/services in the network.

With the identities in place, the devices need to be aware of the services/peers they need to interact with as well as their identities. In some cases, it might be enough to know that any peer with a certificate from a trusted certificate authority (CA) is a trusted peer, while in other cases only specific identifiers should be trusted. Furthermore, different peers/services might have different levels of trust, or the device should only share certain types of information with certain identified peers/services. This is defined through authorisation policies and access control and this information can be configured to the devices directly or securely over the network using some device management protocol such as LwM2M [9].

When connecting to a peer, the device should authenticate the peer before interacting with it. Here the device verifies that the identity of the peer is one of the trusted ones with which it should interact. Typically, also the peer wants to authenticate the device, resulting in mutual authentication. The authentication is based on the strong identities used by the devices. The Extensible Authentication Protocol (EAP) is one typical authentication protocol, which is primarily targeted towards access authentication, such as a device requesting access from an access point or gateway but it can be applied for other types of authentication as well. EAP supports multiple different authentication methods and credential types. Another typical example of mutual authentication is the setup of Transport Layer Security (TLS) with both client side and server side certificates. In the case that the device has 3GPP credentials, it is also possible to utilize them for authentication and key-agreement with the service using the Generic Bootstrapping Architecture (GBA).

Finally, after successful authentication, the device can start interacting with the peer/server. Now it is up to the security policy to define the level of security required by the communication. Even if the access network might itself provide secured access, the communication should ideally be protected end-to-end rather than hop-by-hop. In most cases confidentiality protection, i.e. encryption, is a default choice, especially in smart grid type of scenarios. Encrypted data without integrity protection can however in many cases be modified on the path by an attacker without the receiver noticing it. Typically, the attacker can only achieve random modification of the plaintext, but not choose the exact modification. The more the attacker knows about the plaintext the more he can target the change to a specific part of it. Assuming the plaintext has

well defined format and expected value ranges (e.g. reported temperature or power consumption), the receiver can sometimes notice these types of attacks if the random modifications result in unrealistic values or corrupted message formats. However, explicit integrity protection should ideally be used, e.g. by applying keyed hashes, MACs or digital signatures. Replay protection is also an important feature, which in many cases is provided by the protocols themselves. If this is not the case, it should also be explicitly applied. Protocols for applying communication security include (D)TLS, object security and IPsec. For all of them it is possible to select different algorithms and cipher suites according to requirements. The key material used for securing the communication is typically either based on the authentication keys or negotiated as part of the authentication procedure.

By applying these principles of having a strong identity, proper access control and requiring end-to-end authentication and encryption we can arrive at a good base level of security and many of the threats identified in D1.1 [1], such as man-in-the-middle, eavesdropping and data injection attacks can be efficiently prevented.

2.4.2 Physical Security

In addition to the communications security discussed in Ch. 2.4.1, another big part of the smart grid security is the physical security of the smart grid nodes. There are nodes located at customer premises to which the customer might have direct access and in addition part of the infrastructure nodes are out in the field in unmanned locations. Furthermore, it is not only the node itself that needs to be protected, but also its power supply and communication capabilities, as disabling either of them would also render the node unavailable.

The physical protection of nodes can include both blocking unauthorized access to them and sensors for identifying perimeter breaches. The sensors can be both for the site and for the node itself, e.g. with sensors sensing the opening of the device enclosure. In addition to signalling breaches of the device enclosure, the device could store a state related to this. To protect against tampering of this state it could be stored in hardware secured memory, e.g. in a trusted platform module (TPM). The node's state can then be queried remotely using a remote attestation service, and the state stored in the TPM would be part of the state of the node. The TPM could also be used for storing the credentials and other security critical parameters of the node so that an attacker cannot copy/clone them. Also, other hardware secured modules, such as the universal integrated circuit card (UICC), better known as the SIM card, could be used for storing credentials.

2.4.3 Other Security Measures

In addition to what has already been discussed, it is of course essential to have well educated staff familiar with the underlying systems as well as proper security policies for how they are allowed to behave and access data and nodes in the network. This should also be combined with logs providing non-repudiation.

It is also good to define in advance countermeasures for handling identifiable possible security risks/incidents. This also requires that these incidents can be identified which means that the network and its nodes need to be monitored. The network monitoring centre gathers information about node and network state and actions in the network and alerts the administrator of any abnormal behaviour. This could be e.g. a node firmware being updated without the update being scheduled in the system, which could be an indication of an attack on the node. Based on these alerts, the administrator investigates the cause and potentially performs countermeasures to fix the problems and minimise the effect of them to the network.

Furthermore, up-to-date software, such as OS, firmware and applications, should be maintained in all nodes. For the most critical nodes, hardening of the software might also be a good precaution. Also, anti-virus programs, firewalls and possibly deep packet inspection (DPI) should be installed in the nodes and networks to protect against network and malware types of attacks, such as viruses as identified in D1.1. Other isolation techniques, such as virtualisation and SDN, could be applied as well to shield the nodes and the smart grid network from the public networks as well as node internal functions from each other. By promptly applying updates, potential bugs in the software can be removed, eliminating unforeseen vulnerabilities.

Also, the used cipher suites and security algorithms should be updated if it is found out that there are some weaknesses to them or they have been broken.

The most critical nodes in the network should be duplicated for resilience. In case of malfunction, attacks or accidents the network should be able to continue functioning even when a node is not available, which can be achieved by having a backup node that can handle the critical functions of the disabled node.

2.5 DSO Security Monitoring Centre

The DSO Security Monitoring Centre (DSOSMC) is able to offer a list of countermeasures available for a given threat among the available ones for the specific smart meter application scenario. The DSOSMC harnesses the power of FIWARE platform (https://www.fiware.org/) which is based on software components called Generic Enablers (GEs). Each module defined within the DSOSMC will be developed in the appropriate FIWARE GEs along with protocols and interfaces for operation and communication. This information will be specified in deliverable D3.4 [3] and updated versions of it for the complete match between DSOSMC and FIWARE framework.

DSOSMC forwards the data it receives from NORM to the DE-SMIS after processing it as described in the sub-chapters below. As DSOSMC and DE-SMIS are located at the same TSO/DSO within the same network, they can share data without it being anonymised. In addition, DSOSMC informs DE-SMIS of threats which have been identified by DSOSMC and the selected countermeasures. The functional architecture of DSOSMC is shown in Figure 10 and the functions described in the sub-chapters below.

2.5.1 Monitor Module

The monitor module is responsible for selection of data and pre-processing of the selected data set. It collects data from NORMs and with the threats list obtained from T1.3 performs a pre-processing of the data. This Monitor module is able to adapt and align to different data formats. Depending on the application needs, the data might be collected in various time steps and averaging periods.

2.5.2 Analytics Module

This module performs Transformation of the data and realises Mining processes. This module is a data analytics tool that allows for multi-criteria analysis and detection of spatio-temporal patterns playing a very important role for the optimal management of both Threats identification and Countermeasure selection. In order to identify the Threat and select the countermeasure this component can use one of some concrete and fully fledged algorithmic techniques that allow anomaly detection.

The tool is especially interested in the analysis of patterns with the aim to alert and trigger the proper strategies/operations though a holistic approach that is considered for the whole functionality of the tool. This analytics module is able to detect anomalous behaviour and send this information to other components inside DSOSMC but also to the DE-SMIS.

2.5.3 Countermeasures Extraction Tool Module

The **Countermeasures Extraction Tool** receives as input the list of possible threats and, using the output of the **Analytics** module, provides a list of possible countermeasures and mitigation probability associated to each possible threat detected. It provides both the **Semantically Enhanced Countermeasures** and the **Countermeasure Knowledge Database** with a list of possible countermeasures and mitigation actions.

2.5.4 Semantically Enhanced Countermeasures Module

This module is in charge to select, supported by performance indicators, the best countermeasure to be applied through the Dashboard of DSO monitoring centre and to populate

the **Countermeasures Knowledgebase Database**. The Semantically Enhanced Countermeasures aimed to perform the identification and matching of innovative countermeasures against new and old threats related to smart meter and electrical devices at NAN level.

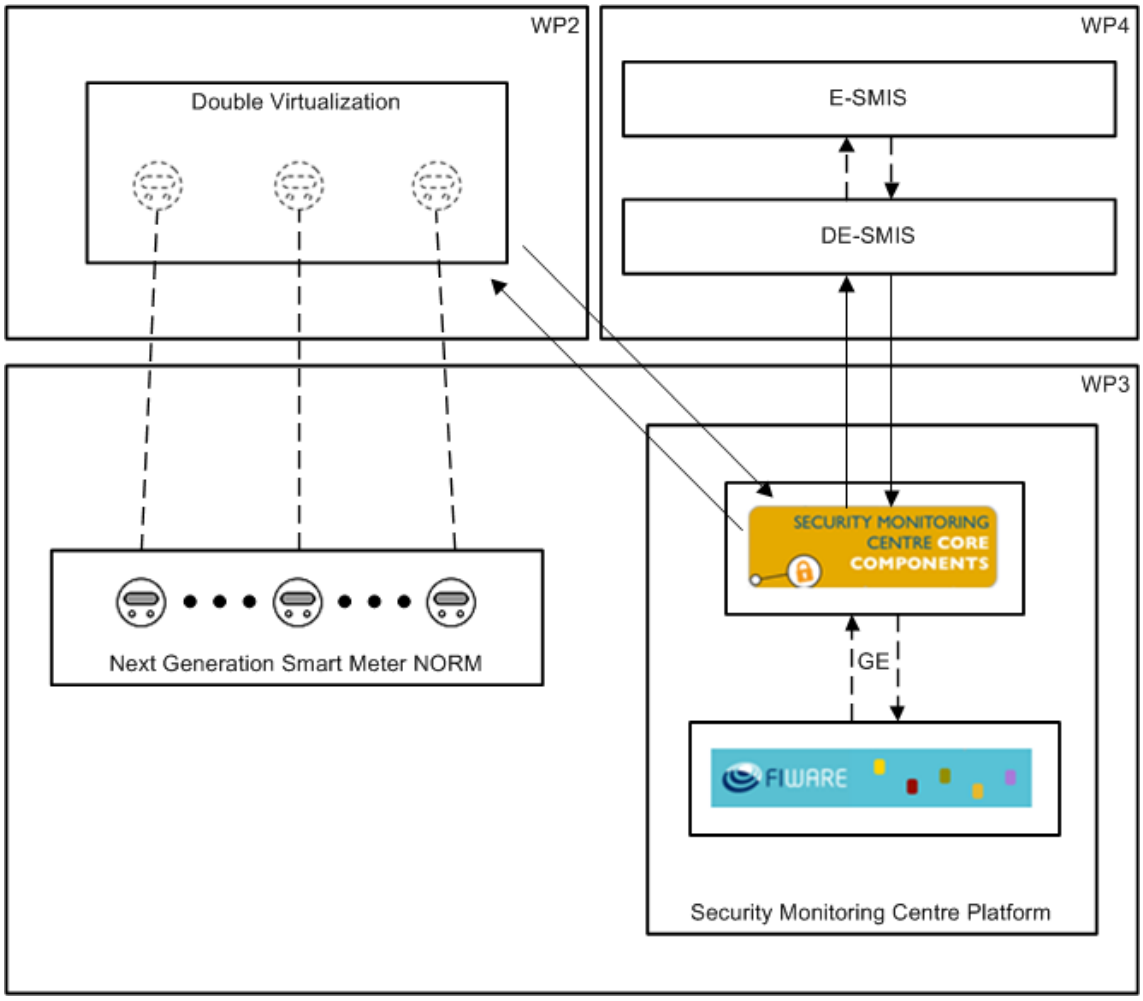

Figure 10: Conceptual Architecture of the DSO Security Monitoring Centre

2.6 Pan-European Security Monitoring Centre

The Pan-European Security Monitoring Centre (ESMC) monitors the security status of critical infrastructure. The system consists of two components:

- Several instances of a decentralized European Security Monitoring and Information System (DE-SMIS) locally collect data on DSO/TSO level.
- The European Security Monitoring and Information System (E-SMIS) collects data from several DE-SMIS instances across Europe. E-SMIS (1) evaluates the data with regard to common patterns, such as cyberattacks and (2) shares the information with DE-SMIS instances.

The combination of E-SMIS and several DE-SMIS instances ensures that DSOs and TSOs obtain information that cannot be derived from their network.

ESMC is shown in Figure 11. It consists of DE-SMIS at the DSO/TSO level and E-SMIS at the European level. To identify new patterns, DE-SMIS receives data from
(1) E-SMIS by Interface I5,
(2) DSOSMC by Interface I3, and

(3) further sources by Interface I7.
In particular, DSOSMC is only one data source among many for DE-SMIS.

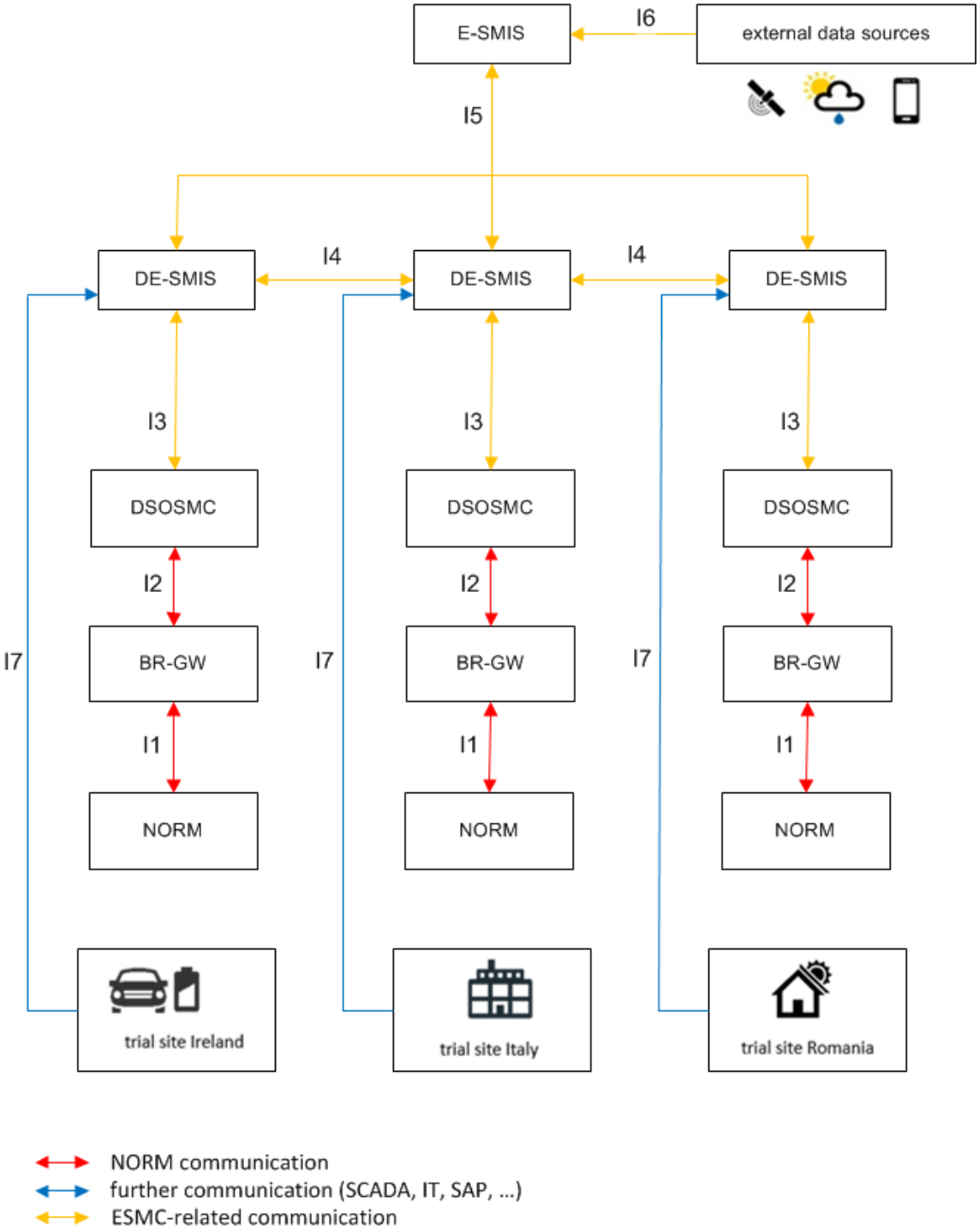

Figure 11: Overview of the Infrastructure of ESMC

2.6.1 Infrastructure

Figure 11 gives an overview of the infrastructure of ESMC. ESMC consists of one central instance E-SMIS that is responsible for the pan-European view. At this level, external data sources, such as weather data, geographic or social media data, are incorporated to the monitoring centre for a comprehensive view on critical infrastructure. For example, it can be

evaluated whether IT-security-related twitter tweets can be used to predict attacks on critical infrastructure.

Moreover, the centralized E-SMIS instance obtains information from several decentralized instances (DE-SMIS) which lie on the level of DSO/TSO. The rationale for establishing DE-SMIS instances is that they

1) collect, aggregate and analyse locally bounded data. Hence, DE-SMIS reduces traffic by ensuring that only significant security-related information is shared with E-SMIS.
2) make the collected data anonymous. Typically, the data at DSO/TSO level have various legal restrictions due to privacy issues, such that an anonymisation step is crucial for data sharing.

DE-SMIS instances share information, such that the E-SMIS can produce an aggregate analysis on a European level. Thus, it becomes possible to detect patterns which cannot be evaluated on local DSO/TSO level. The E-SMIS in return shares the analysis results with DE-SMIS instances. Thereby, the DE-SMIS instances can confirm the patterns by comparing them with the data available in their own network.

ESMC searches for unexpected and significant patterns in data which stem from various sources. In case such a pattern has been detected successfully, ESMC

1) precisely visualises the results for reasonable human-machine interactions. The visualisation concept depends on the structure of the data (e.g. streaming or event based data transmission) which will be transmitted to the ESMC. Particularly, time resolution and the amount of data will determine the underlying visualisation approach.
2) notifies the responsible authorities such that proper countermeasures can be initiated in a downstream process by the controller.

On the contrary, the DSOSMC centre will perform countermeasure selection and application in an automatized way (see Ch. 2.5).

2.6.2 Communication

Local DE-SMIS instances communicate with agents. Agents are linked to exactly one data source and ensure a secure data sharing with DE-SMIS. Data sources can be IT-related systems such as firewall, SIEM (Security Information and Event Management) systems and IDS (Intrusion Detecting System) or energy-related systems such as SCADA system. In particular, the DSO Security Monitoring Centre is an agent of DE-SMIS which provides pre-processing information about threats and countermeasures for critical infrastructure. See Ch. 2.5 for details about the DSO Security Monitoring Centre.

Moreover, DE-SMIS instances shall be able to communicate with each other. This communication can be established at a local or national level and serves multiple purposes. The rationale is that threat patterns and attacks identified by a DE-SMIS instance based on its own data are directly shared with other DE-SMIS instances. DE-SMIS instances shall be able to increase the efficiency of their search since they will be able to test their own (private) data on the threat patterns from the adjacent DE-SMIS. This kind of communication does not require any significant resource allocation for data processing for the receiving DE-SMIS, therefore the analysis and the comparisons can be conducted quickly and efficiently. These immediate notifications and early warnings sent by a DE-SMIS instance that has identified a threat pattern can prevent geographically correlated attacks to adjacent DE-SMIS instances which is usually the case in recent attacks on multiple DSOs. The latter is stated at the study of the Ecossian Project, supporting the need for communication between local Critical Infrastructures [10].

A fallback mode for the communication between the DE-SMIS instances may be triggered in case the E-SMIS is inaccessible due to malfunction, maintenance or an attack. In this mode, a DE-SMIS shares all its public data with the DE-SMIS instances, as would do with the E-SMIS in the normal mode. The receiving DE-SMIS instances compare these data with their own private data and identify common threat patterns and attacks on regional level. The DE-SMIS

communication functionality and the data processing on the DE-SMIS level resemble, in this case, the communication between DE-SMIS and E-SMIS. Although time- and resource-inefficient for the DE-SMIS, this mode mitigates the impact of an attack or a malfunction on the E-SMIS, since the DE-SMIS are still able to communicate with each other and identify threat patterns on a large scale. Therefore, the existence of this mode is necessary within the concept of enhanced security and availability at the E-SMIS level.

2.6.3 Relationship between DE-SMIS and DSOSMC

DE-SMIS obtains data from various data sources, including IT-related data such as firewall log files and energy-related data such as SCADA log files. In particular, DE-SMIS receives data from the local DSOSMC instance at the DSO/TSO level which contains information about the identified threats, the initiated countermeasures and measurements from the NORM devices (Interface 3, see Ch. 2.7.3). Data provided by DSOSMC is only one data source among many for DE-SMIS. At the DSO/TSO level, DE-SMIS and DSOSMC work in a 1:1 relationship.

2.7 Interfaces in the success Security Monitoring Solution

As depicted in Figure 2, the success Security Monitoring Solution comprises various devices which exchange information through the depicted interfaces. These interfaces define which data is shared.

2.7.1 I1 between NORM and BR-GW or DSOSMC

The I1 interface provides connectivity between NORM and BR-GW or, in configurations without BR-GW, between NORM and DSOSMC. All the information between the rest of the other components (E-SMIS, power system applications) and NORM will be exchanged over this interface.

2.7.2 I2 between BR-GW and DSOSMC

Once the threat countermeasures analysis has been accomplished and the part of the network and the devices with suspicious behaviour have been identified with some probability, the DSOSMC component is in charge of selecting the best countermeasure among the available ones in order to solve as much as possible the identified violations.

Possible countermeasures are to communicate information on compromised devices and detected anomalies in pattern to the BR-GW. This information is communicated to the BR-GW. The same is possible in the other direction, that BR-GW can detect security anomalies and send alarms on them to the DSOSMC. Hence, there is a bidirectional exchange of data over interface I2 as shown in Figure 2. The functions described in Ch. 2.3.1 such as Data Centric Security will notify DSOSMC over this particular interface

2.7.3 I3 between DSO Security Monitoring Centre and DE-SMIS

Countermeasures related to attacks through the Neighbourhood Area Network (NAN) zone are addressed by DSOSMC. Its toolbox matches and correlates potential new and old threats (with high impact and risks detected within WP1), with the most suitable security actions and countermeasures for the specific application scenario related to NAN-level smart devices.

DSOSMC selects countermeasures such that a countermeasures repository will be incrementally populated. DSOSMC will share information about the detected threats, the initiated countermeasures as well as pre-processed NORM features with DE-SMIS. At TSO/DSO level, DSOSMC and DE-SMIS interwork in a 1:1 relationship where DSOSMC provides one among many data sources for DE-SMIS.

To fully understand how the DSO Security Monitoring Centre will make available to DE-SMIS the countermeasures information it is useful to underline the intertwined process of threat and countermeasures management. With this aim in fact will be provided a first model of the conceptual architecture of the DSO Security Monitoring Centre depicted in Figure 10.

2.7.4 I4 between DE-SMIS instances

The interface I4 between the different DE-SMIS shall comprise information and attack patterns that the DE-SMIS has detected as threat relevant, so that an immediate response can be initiated by all DE-SMIS that could potentially be under attack, as explained in Ch. 2.6.2. The criticality of a DSO's response to an imminent attack makes the communication between the DE-SMIS very important, since the data process at the E-SMIS domain might not meet the stringent time requirements. The interface I4 enables also the DE-SMIS which receive the attack patterns to compare these patterns with their own private data and draw more efficiently conclusions about their current status. Note that the DE-SMIS share with the E-SMIS a larger amount of data than they share with the DE-SMIS. This is due to the fact that the E-SMIS uses the DE-SMIS public data to detect threats on a larger level than what each DE-SMIS could possibly do by combining its private data and the public data of any other DE-SMIS.

Furthermore, the interface between the DE-SMIS could substitute interface I5 in the emergency case when the E-SMIS may not be operational, which would initiate the fallback mode described in Ch. 2.6.2. This mode also stresses the importance of interface I4 within the success solution, as it provides a decentralised and more fault-tolerant approach to the security monitoring system.

Similarly, as in the interface 5, this information needs anonymisation towards creating a privacy firewall between the different DE-SMIS entities.

2.7.5 I5 between DE-SMIS and E-SMIS

Interface 5 (I5) in Figure 2 comprises the exchange between E-SMIS and its corresponding DE-SMIS instances.

As described in Ch. 2.6.1, the data on the DE-SMIS are in the domain of the DSO/TSO. Thus, the processing of these data can include information the DSO/TSO has from his own network. As part of the interface I5, the DE-SMIS performs an anonymisation and any further necessary aggregative processing in order to create a privacy barrier/firewall to ensure that the E-SMIS (and the rest of the DE-SMIS instances at the respective interfaces I4) does not have access and cannot deduce any secondary/private information regarding the underlying data. Interface 5 thus separates the E-SMIS data domain from the DE-SMIS data domain. The E-SMIS data domain can be considered as "public" within the ESMC system, since the E-SMIS aggregates and processes the data and patterns from all DE-SMIS, including open data from external sources. On the contrary, the DE-SMIS data domain is the "private" data domain for each DSO/TSO.

The data that the DE-SMIS shares with the E-SMIS includes pattern-specific data, even if the DSOSMC cannot detect any significant abnormalities and of course any further identified attacks/threats.

The E-SMIS will share through I5 any identified patterns, weighted with the results from external data sources (see Ch. 2.7.6). Since these data comprise information that is "public", the E-SMIS part of I5 does not need a further anonymisation process.

2.7.6 I6 between E-SMIS and External Data Sources

Interface 6 in Figure 2 comprises the communication content between E-SMIS and external data sources.

External data sources may vary significantly in the type of data that they may provide. For example, at the current stage of development, it is being examined whether social media can provide meaningful data. Such messages could be analysed at the pan-European level concerning issues that are relevant for IT-Security in critical infrastructures. Interface 6 must ensure that the data from these sources are processed and filtered adequately.

Hence, social media analysis is performed by E-SMIS and the results are shared with DE-SMIS instances by Interface 5 (see Ch. 2.7.5).

2.7.7 I7 between DE-SMIS and internal data sources

DE-SMIS can further receive data from internal data sources by Interface 7 in Figure 2. This data is called internal since they are within the DSO/TSO data domain, thus they are DE-SMIS private data. Such data can potentially stem from (1) energy-related sources such as SCADA systems and control room software; and (2) IT-security sources such as SIEM systems, firewalls or antivirus scanners. The functionality of interface 7 focuses on extracting the necessary content, similar to the functionality of interface 6.

2.8 Double Virtualisation

In order to increase the resiliency of the power system, a double virtualisation logic will be applied. The concept is that the functions and the devices' representation on the Cloud platform infrastructure will be deployed in separated logical layers, called the Functional and Data Layer (see Figure 12). The Functional Layer contains the virtual instances where the power system monitoring and control applications are deployed, while in the Data Layer are hosted the so-called Virtual Devices, virtual representation of measurement devices installed in the field (e.g. Smart Meters or PMUs).

The example Cloud infrastructure shown in Figure 12 is contained in a so-called Flight Box, which is a test rack containing an Openstack-based cloud infrastructure and a 4G mobile eNodeB, which will be made available by Ericsson and used in the RWTH ACS Lab for tests of double virtualisation in success WP2.

Note that in terms of the success Infrastructure model of Figure 1, the concept is applicable on the Application layer: when applying double virtualisation, a system on the Application layer of Figure 1 is separated into functional and data-related parts.

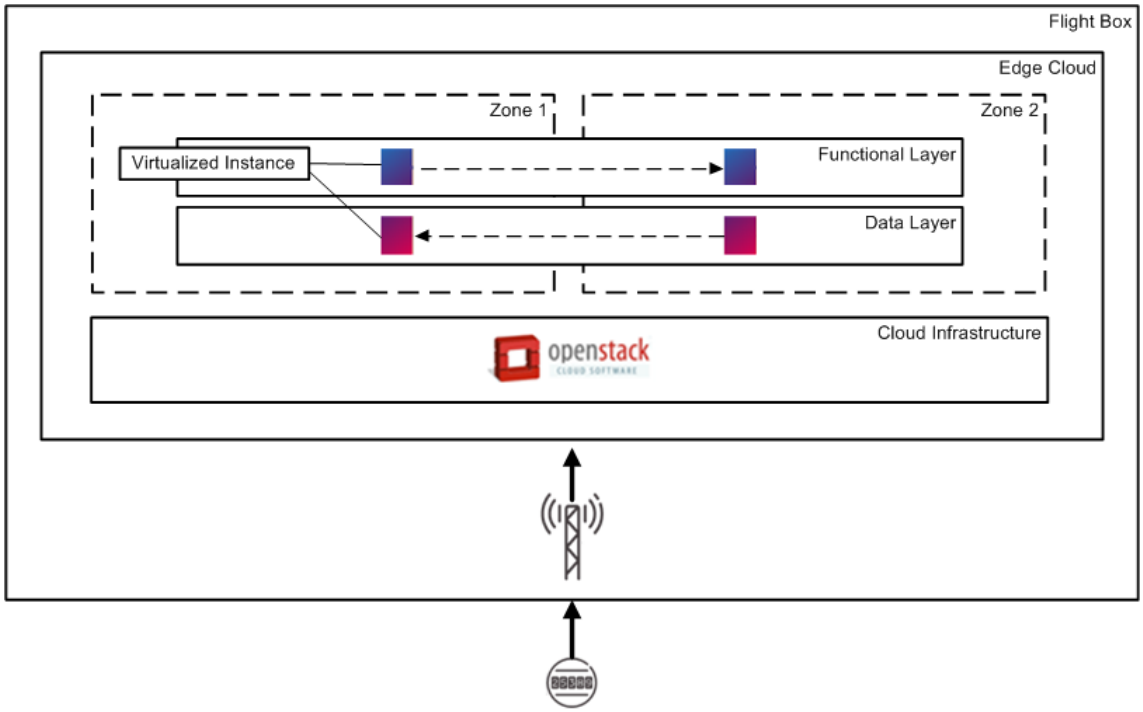

Figure 12 Double Virtualisation Principles

A minimum of two zones will be defined that will be logically and/or physically separated. E.g. zones can belong to different networks or they can be deployed in different physical servers.

The virtualisation of the power system applications in the Functional Layer aims at reinforcing the resiliency of success architecture by allowing the migration of the applications to a new safe zone when the security and integrity of the original zone is compromised. It is also possible to start up a new virtual instance, instead of just migrating the original one, in case the attack strikes at the virtual machine itself, thus neutralising the attack when switching off the affected virtual machine.

The virtualisation of the field devices' representation, on the other hand, has the main purpose of hiding the physical devices installed in the field behind their virtual representations. By doing this, the only exposed entities will be the virtual devices and any attack aiming at the devices will impact these virtual devices. When an attack is detected, it can be isolated by deactivating the connection between the physical and the virtual device. A new virtual device instance is then started up in a new zone and the connection with the physical device restored, while the attack is neutralised by switching off the compromised virtual instance.

When a cyber-attack is detected, either from an external or an internal network, virtual instances will be immediately migrated to another zone. Streaming of the data can be temporarily delayed during the migration but all data will be processed.

The functional and data layers, which will contain functional and data entities, will be logically separated. In case of the attack on the separate layer, the relevant entities will be migrated. In case that the attack is targeted at a single layer, its effectiveness will be reduced. Combined attacks targeting simultaneously both layers will be complex to execute, since they will require different approaches and methodologies to be applied at the same time on different targets.

An example of an Application to which virtualisation can be applied is a DEMS application such as State Estimation, where measurements of the voltage levels and phase angles at various points in the electrical grid are used to estimate the electrical grid state. Such a DEMS application would belong in the Application layer of Figure 1. In double virtualisation, the State Estimation would be realised with functional and data-related parts running on separate VMs which can be moved as a countermeasure to a security attack.

3. List of Countermeasures

The security configuration and measures discussed in Ch. 2.3 provide a good basic security for the smart grid and eliminate many attacks identified in D1.1 [1] on the communication, the network and the physical devices. However, no system is bulletproof, and as such it must be prepared for the event of a security incident. Security is not only about cryptographic algorithms and their application in various tasks. Security covers also attack detection. However, if the adversary can manoeuvre around all security obstacles laid out in the architecture, there is nothing to be done. Therefore, having proper security by design in place is like having security obstacles all around the architecture complementing each other so that no attacker can by-pass all of them. Once any single obstacle is tripped, a security incident can be confirmed, and reacted to.

Identification of security incidents can be achieved by monitoring the network and the nodes in it. If a node suddenly is not reachable/available, it is a clear signal that something is not right with the network. However, it is difficult to say exactly what has happened, it could be a physical attack on the node, a network based attack/hack on the node (e.g. Denial of Service (DoS) attack) or a natural disaster or accident that has destroyed the node. Also, any abnormal behaviour could be a signal of an attack or malicious intent.

Once a security incident has been detected, it should be mitigated by following a pre-defined procedure, consisting of a number of steps or parts. This mitigation procedure is referred to as a "countermeasure".

The following list contains countermeasures to incidents that are (easily) detectable. Assuming the security solution of Ch. 2.3 is applied, e.g. noticing that the credentials of a node have been leaked and are used for performing man-in-the-middle attacks is very difficult and it might well be that the attacker can utilize them for a long period of time before there is any indication of

that the credentials have been leaked and misused. Therefore, these types of incidents and associated countermeasures are not included in the list, at least for now. Most of the countermeasures require at least some form of human interaction, e.g. in the form of accepting/authorizing the system to perform certain steps of the countermeasures and sometimes even requiring the human user to initiate some process that are part of the countermeasures.

Table 1: Incidents and Countermeasures

Incident Label	Incident Description	Countermeasure
I-1	Perimeter breached	1. Alert security personnel to the location (infrastructure node)
I-2	Device casing breached	1. Alert security personnel to the location (infrastructure node) 2. Remote attestation of device state 3. Send maintenance unit to location a. Reset device & re-bootstrap (new credentials & revoke old ones) b. Repair device c. Replace device
I-3	Communication link unavailable	1. Re-configure network to route node via secondary access (if available) 2. Send maintenance unit to location a. Reset network connection & unit b. Repair network connection & unit c. Replace network connection unit
I-4	Device power unavailable	1. Enable backup power 2. Send maintenance unit to location a. Reset power supply unit b. Repair power supply unit c. Replace power-supply unit
I-5	Device unavailable	1. Enable backup node if available 2. Send maintenance unit to location 3. Reset device & re-bootstrap (new credentials & revoke old ones) 4. Repair device 5. Replace device

I-6	Security algorithm deemed insecure	1. Select and review proper alternative algorithm 2. Remotely configure affected nodes to deprecate insecure algorithm and enable alternative algorithm
I-7	Device behaving suspiciously	1. Perform remote attestation to verify device state 2. If state is OK, red-flag the device a. Temporarily disconnect device from the grid b. Investigate
I-8	Remote attestation fails (after step 1 of I-7 above)	1. Disconnect device from the grid. 2. Send maintenance unit to location 3. Reset/Reinstall device & re-bootstrap (new credentials & revoke old ones)
I-9	Unauthorized messages	1. Identify node or network segment where data is originating 2. If node, perform I-7 3. If network segment, it means there is an unauthorized node in the network segment 4. Isolate network segment 5. Investigate
I-10	Virus detected in node	1. Isolate node from network 2. Enable backup node if available 3. Reinstall device to remove malware 4. Verify peers not infected 5. Update malware definitions in all nodes as soon as possible
I-11	DoS suspicion	1. Block DoS traffic at edge of network by updating firewall rules 2. Enable backup node if available 3. Do load-balancing if possible 4. Analyse suspected DoS traffic, verify attack

The countermeasures defined in Table 1 do not cover double virtualisation (see. Ch. 2.8). Double virtualisation can be applied for incidents I-9 and I-10 and the action is to move the data or applications to another physical/logical zone.

A mapping showing how the countermeasures map to the threats identified in deliverable 1.1 is shown in Table 2 in Ch. 15.

4. Countermeasure for Incident I-1

4.1 Description

Incident name: Perimeter breached

Incident characteristics: Unauthorized access to a site. The site surveillance equipment, e.g. motion sensor, notices non-approved physical action or presence.

Root cause: An unauthorized person accesses the site and triggers at least one of the monitoring equipment surveilling the site.

Incident identification: An alarm is raised at the monitoring centre indicating the site and what has been observed. Security personnel is dispatched to the site to verify that everything is OK, or handle any situation that has occurred.

4.2 Related SW Functions

None.

4.3 Related Infrastructure

None.

5. Countermeasure for Incident I-2

5.1 Description

Incident name: Device casing breached

Incident characteristics: The casing of a node or end-device is opened without authorisation. A sensor inside the device monitors the state of the case and signals whenever it is opened.

Root cause: Someone tries to open the case, possibly to try to modify the device e.g. to report wrongful meter readings.

Incident identification: An alarm is raised at the monitoring centre indicating the node where the casing has been breached. If the incident is at an infrastructure node, security personnel is dispatched to the site as in Incident I-1. For end-devices this step can be skipped. Then, remote attestation is performed to verify the device state. Once security personnel have verified site integrity, a maintenance person can be sent to the site if deemed necessary (based on visual observation and/or remote attestation result). The maintenance person should reset and re-bootstrap the node to generate new credentials for it and getting those credentials properly configured to the backend/system. If needed, the device should be repaired or even replaced if required. The same maintenance steps should be taken also for end-devices. Maintenance fees should fall on the owner of the end-device if device located in owner premises.

5.2 Related SW Functions

At the level of NORM, a micro-switch will be considered to monitor the housing of NORM, which should be read by the Energy Gateway of NORM and sent as alert message to the Security Agent running in the Energy Gateway, event which need to be sent to the DSOSMC.

5.3 Related Infrastructure

As presented in Ch. 5.2, the NORM housing will have a micro-switch to monitor eventual opening and intrusion inside for having NORM hardware access.

6. Countermeasure for Incident I-3

6.1 Description

Incident name: Communication link unavailable

Incident characteristics: The node's communication link is unavailable, i.e. the node cannot be reached and it cannot communicate with others. Looks like node is not available.

Root cause: For this incident characteristics, multiple incidents are possible (Incident I-3 – Incident I-5). For Incident I-3, the reason for not being reachable is that the communication link of the node is not functioning.

Incident identification: The node does not communicate according to communication pattern (i.e. if we expect to see a message and we do not see it) and cannot be connected to e.g. to perform remote attestation. If available, an attempt can be made to enable secondary/backup communication link of the node. If this is not successful it is likely that the incident is actually either Incident I-4 or Incident I-5. Next, a maintenance unit should be sent to the site to fix the issue. Initially a reset of the communications unit could help, otherwise it needs to be repaired or even replaced.

6.2 Related SW Functions

None.

6.3 Related Infrastructure

None.

7. Countermeasure for Incident I-4

7.1 Description

Incident name: Device power unavailable

Incident characteristics: Node's power is not available, node cannot operate. Looks like node is not available.

Root cause: For this incident characteristics multiple incidents are possible (Incident I-3 – Incident I-5). For Incident I-4, the reason for not being reachable is that the node has lost its power.

Incident identification: Node does not communicate according to communication pattern (i.e. if we expect to see a message and we do not see it) and cannot be connected to e.g. to perform remote attestation. As the power is out, enabling the secondary communications link as in Incident I-3 will not work. Next, enabling of possibly available backup power can be attempted. If not successful, the incident is most likely of type Incident I-5. Next, a maintenance unit should be sent to the site to fix the issue. Initially a reset of the power supply unit could help, otherwise it needs to be repaired or even replaced.

7.2 Related SW Functions

None.

7.3 Related Infrastructure

At NORM level, due to economic reasons, usually there is no backup supply, to allow functioning when network voltages are missing. This backup solution may exist only in resilient nodes, where power supply for critical loads is in place, based on UPS or other resilient architectures include energy storage.

8. Countermeasure for Incident I-5

8.1 Description

Incident name: Device unavailable

Incident characteristics: Node is malfunctioning and will not operate. Looks like node is not available.

Root cause: For this incident characteristics, multiple incidents are possible (Incident I-3 – Incident I-5). For Incident I-5, the reason for not being reachable is that the node is malfunctioning.

Incident identification: Node does not communicate according to communication pattern (i.e. if we expect to see a message and we do not see it) and cannot be connected to e.g. to perform remote attestation. As the node is malfunctioning, enabling the secondary communications link as in Incident I-3 or backup power as in Incident I-4 will not work. To maintain optimal network operation a backup node should be enabled if available to take on the role of the faulty unit. Next, a maintenance unit should be sent to the site to take care of the node. An attempt to reset and re-bootstrap the node could be done, but if not successfully recovered, the node would have to be repaired or even replaced.

8.2 Related SW Functions

None.

8.3 Related Infrastructure

None.

9. Countermeasure for Incident I-6

9.1 Description

Incident name: Security algorithm deemed insecure

Incident characteristics: Academia, standardisation organisations or other authority states that a security algorithm deployed and used in the network is insecure and should be deprecated.

Root cause: Some entity has found a weakness in either an algorithm or a specific implementation of an algorithm.

Incident identification: Reliable publication of affected algorithm and proof of weakness. If the weakness is serious and could affect operations, a suitable replacement algorithm needs to be found and analysed. Once the new algorithm is approved, it needs to be installed in all places where the old (vulnerable) algorithm was used. If possible, this should/could be done remotely.

9.2 Related SW Functions

The cryptographic library that implements and provides the affected vulnerable algorithm needs to be updated and/or the node(s) using it needs to be re-configured to not use the affected algorithm.

9.3 Related Infrastructure

Any node in the system that uses cryptographic functions might be affected depending on if they have been configured to use the affected library or vulnerable algorithm.

For NORM, in specific cases when deployed security algorithm need more computational power or need changes in the HW which assist the security functionality (e.g. related to hardware needed to implement the PUF), the new algorithms may ask also for hardware upgrades. The Unbundled Smart Meter (USM) concept allows that both hardware and software upgrades can be made without affecting the hardware and functionality of the Smart Meter and of the PMU, as components which communicate with the Energy Gateway.

10. Countermeasure for Incident I-7

10.1 Description

Incident name: Device behaving suspiciously

Incident characteristics: The threat, or incident, to which this countermeasure is applied is when a device in the network behaves suspiciously. This can mean that a device communication pattern does not match the typical one for a device of this type e.g. with respect to the frequency of messages, size of message, communication peer, i.e. to many or few packets, possibly sent too often or seldom either to expected or unexpected peers. Likewise, this threat relates to the content of the communication either by having the device provide data that is outside the normal range and thresholds defined for the device type or even by having the data be of unexpected type.

Root cause: The cause for these suspicious behaviours, if indeed erroneous, can stem from one of two things; the device is behaving strangely because of a bug or configuration error, or the node or its credentials have been compromised. The software of devices in the network should be updated regularly to remove found vulnerabilities or other unwanted features and to add new functionality to add value. Software here means anything from firmware to operating system, drivers, applications and configurations. Even when these are updated/modified with good intent, it is possible that it results in unwanted behaviour due to bugs or erroneous configurations. Depending on the severity of the bug/misconfiguration, detecting it might not be easy, e.g. if it results in measurements being off by only a small margin. Also, hardware bugs/breakdowns are possible and can result in similar behaviour.

The other alternative for a node behaving suspiciously is if an attacker has managed to gain control of the device or its credentials. This is typically catered for by having security flaws in the device software that the attacker can abuse for gaining unauthorized access. This then links back to the previous paragraph and the need to update the software of the device. Assuming the security measures discussed in Ch. 2.4 have been implemented the only way an attacker can produce legitimate looking data is by gaining access to the device and/or its credentials. With end-to-end security applied, an attacker will not be able to inject data or generate own valid looking messages without approved credentials. Depending on how the attacker acts with the compromised node/credentials, identifying the incident/actions might be anything from easy to impossible.

Incident identification: Identification of these incidents is done by having the monitoring centre verifying traffic in the network against accepted/expected traffic patterns. When the traffic differs from the expected more than a set threshold it is an indication that the incident has occurred and the appropriate countermeasures should be taken. The analysis of the devices' traffic is performed by DSOSMC and DE-SMIS at the DSO/TSO level. As described in Ch. 2.5 and Ch. 2.7,, DSOSMC provides certain data features such as RAM usage to DE-SMIS. DE-SMIS correlates this information with information from other sources (see Chs. 2.7.5 and 2.7.6) to extract new findings about the system's status.

After the incident identification, remote attestation should be performed on the suspiciously behaving node. This will verify the state of the node and can find indications of compromising of devices. In Incident I-7, we assume the attestation does not fail, i.e. the device state is OK. Thus, the device should be red-flagged, indicating there is an unresolved issue with it, and it should be isolated from the network pending further investigation.

10.2 Related SW Functions

From the Communication perspective, the Data centric security function in BR-GW described in Ch. 2.3.1 can be utilized to verify the state of the device. During device deployment, a signature based on device parameters is generated from data centric security function. This signature is taken as base for verifying state of device in real-time. Whenever the signature differs from the

base signature taken during deployment, the BR-GW can take action to block the traffic originating from that device. Also, it can be further can be used to notify DSOSMC regarding status of infected device.

DSOSMC performs for online monitoring of network traffic, deduction of usual behaviour and detection of suspicious behaviour (e.g., through threshold alerting when exceeding normal traffic levels deduced from historic monitoring data). When a suspicious behaviour is detected this information is addressed to DE-SMIS which executes a meta-analysis.

10.3 Related Infrastructure

Once DSOSMC has detected a security violation, it can communicate to BR-GW that one or more NORMs are compromised and have to be disconnected.

DE-SMIS at TSO/DSO level receives data from DSOSMC and combines them with further data sources such as firewall logs (see Figure 11) to extract new findings about the systems status. Therefore, DE-SMIS is able to generate a holistic view of the system to red-flag devices which cannot be trusted any more. After red-flagging the device, DE-SMIS shares the potential finding with E-SMIS. E-SMIS then searches on a pan-European level for significant patterns which indicate an attack. All new findings obtained by E-SMIS or DE-SMIS can potentially lead to a new strategy how to red-flag devices. However, how to proceed with these findings and how to implement a new red-flagging strategy is outside the scope of the success project (as mentioned in Ch. 2.2 above).

The cloud environment that applies the Double Virtualisation infrastructure can be used to move the attacked virtual instances to another physical or logical entity. The moving process can be a thoroughly automatised process. E.g. attacked data can be moved to another server or IP network. The implementation method used for the Double Virtualisation infrastructure considers also decoupling of applications and data. In fact, the data coming from the field devices is stored in a dedicated virtual machine managing only the data storage. In this way, the migration of both applications and virtual devices will be easier and faster, since it will not require also the migration of a large number of historical datasets.

11. Countermeasure for Incident I-8

11.1 Description

Incident name: Remote attestation fails

Incident characteristics: This incident is an alternative branch of the flow of Incident I-7, and relates to the situation where the remote attestation fails for the suspiciously behaving node. This indicates that there is indeed something wrong with the node.

Root cause: The fact that the remote attestation fails means that the state of the node is not acceptable, i.e. the node has been modified in some unacceptable way. This could be by malicious action or fault/bug in the system.

Incident identification: Once the remote attestation fails the node is deemed to be compromised and it needs to be immediately isolated from the network. A maintenance unit needs to be sent to the node to reset and re-bootstrap the device. Re-bootstrapping means the device will get new credentials, which is necessary since it is very likely that the device has been compromised by an attacker and the credentials can have been revealed.

11.2 Related SW Functions

In case of failed attestation, BR-GW can put the device in its black list and will not accept traffic from the device anymore. BR- GW informs DSOSMC about the failed node attestation.

11.3 Related Infrastructure

Breakout Gateway, DSOSMC.

DSOSMC shows to the DSO operator a set of possible countermeasures that can be put in place:

- Send a maintenance unit to reset and re-bootstrap the device.
- Disconnect the device from the grid sending information to BR-GW

12. Countermeasure for Incident I-9

12.1 Description

Incident name: Unauthorized messages

Incident characteristics: Network sees unauthorized messages, meaning the messages might not have a (valid) signature or might be of wrong type considering who is sending/receiving the messages.

Root cause: Someone tries to send unauthorized messages, possibly with the intent to disrupt the system or gain information about the system.

Incident identification: Either the monitoring centre notices these unauthorized messages or a node in the system can report to the monitoring centre about the unauthorized messages it sees. The first step is to try to identify the source of these messages, which could be either a node registered in the system or an unauthorized node attached to the system. Based on the source address of the unauthorized messages the node and network segment in which the node resides can be identified. For attacks including spoofing of source address a more detailed analysis of network behaviour and the suspicious flow need to be done to identify the network segment and/or node from where the messages are coming. If the messages are originating from a node in the system, Incident I-7 should be applied on that node to verify its state. If the source of the messages is not part of the system, it means there is an unauthorized node in the network and the network segment from which the node is sending the messages should be isolated to minimize the damage. Finally, the network segment should be investigated to find the unauthorized node, or its point of entry. The result of the investigation should be identification of the node and/or point of entry to the network, and removing the node from the network.

12.2 Related SW Functions

The GBA function described in Ch. 2.3.1 of Breakout Gateway can be utilised for the authenticating the application messages based on SIM card authentication done by cellular network provider. Furthermore, NMF function can check for the unauthorized transmission of packet on a network address. Based on detection of such events, action can be taken by BR-GW to isolate the device from network.

12.3 Related Infrastructure

Breakout Gateway, DSOSMC, DE-SMIS.

If an attack is detected by BR-GW, an alarm will be invoked at the DSOSMC. If DSOSMC cannot detect the attack, it will be left for DE-SMIS to make the decision. DE-SMIS has a wider scope of knowledge and with machine learning algorithm can decide if disconnect the node.

Double Virtualisation infrastructure in the cloud environment.

13. Countermeasure for Incident I-10

13.1 Description

Incident name: Virus detected in node

Incident characteristics: A virus is found in a node either based on antivirus software in the node identifying the virus or monitoring centre identifying communication pattern of a node matching the pattern of a virus infection. Alternatively, the result from investigation in Incident I-7 might show that there is a new malware on the loose, which has affected the node.

Root cause: Malware has found its way to a node.

Incident identification: Once the infection has been identified the node should be isolated from the network to minimize risk for further infections and damage. If available, a backup node should be enabled to maintain full system operation. The infected device should be cleaned of the malware, which is most securely done by reinstalling the device. After the device is cleaned also its peers need to be verified to not have been infected. If the malware is new, i.e. not part of the known malware definitions, it should be added and the definitions should be updated across the system.

13.2 Related SW Functions

If NORM detects any kind of virus or any suspicious activity, then it can inform BR-GW so that BR-GW can take some action on it accordingly. In addition, the Network Monitoring Function described in the Ch. 2.3.1 can detect DoS attack. Once such event is detected, BR-GW can block traffic originating from device. Furthermore, action can be notified to the DSOSMC.

Also, DSOSMC itself detect a successful infection and report it to the DE-SMIS.

13.3 Related Infrastructure

Breakout Gateway, DSOSMC, DE-SMIS.

Double Virtualisation infrastructure in the cloud environment.

14. Countermeasure for Incident I-11

14.1 Description

Incident name: DoS suspicion

Incident characteristics: The system, or a node in the system is targeted in a (D)DoS attack. This typically means that a huge amount of service requests (anything from an echo request (ping) to service specific API requests) are sent to the victim to exhaust its resources. This can be identified by analysing the traffic (abnormal amount of (similar) request to the target) or the state of the node (resources exhausted). The node can itself report on this or some other node in the network can report on the abnormal traffic amount.

Root cause: An attacker wants to disable parts of or the whole system and launches a (D)DoS attack.

Incident identification: When the (D)DoS attack has been identified the associated flows and flow types (e.g. based on message type, protocol, source address and port destination address and port) should be blocked, if possible (it might not be possible to distinguish attack flows from legitimate flows), at the edge of the network so that the attack flow does not have to be processed and forwarded by more nodes than necessary. This can be done by configuring firewalls to block those flows/flow types. If available, a backup node for the attacked node should be enabled to maintain operation of the system. Furthermore, depending on the attack, the load in the network should be distributed to maintain operation. The attack flows should be analysed to verify it is actually an attack (natural disaster or other similar event could result in a lot of traffic being generated in the network).

14.2 Related SW Functions

The Data centric security function described in Ch. 2.3.1 can enable detection of malware insertion at device level. The BR-GW can verify the device integrity by regular checks of the device's log; it can enable check of any unauthorized software insertion at device level (malware). Furthermore, signatures can be updated based for the firmware updates on the device.

The BR-GW, after detecting changes in the device's log using the Data centric security function, can block the traffic originating from device. After such an incident occurs, peers of infected device can be verifying by data centric security function.

In case of a DoS attack on BR-GW itself, SDN technology can handle it and will block the traffic.

The DSOSMC can gather information about traffic from NORM and BR-GW. This information then can be analysed using the analytic module, allowing construction of an immune based memory which allows classification of, and dynamical reflection of changes in, the analysed data. It sends this information to DE-SMIS to eventually put in place a countermeasure to block the illegitimate traffic flows.

If the E-SMIS is targeted in a (D)DoS attack, it is incapable of receiving the public data from the DE-SMIS and external sources and sending back data with identified threat patterns. The fallback operation mode of the DE-SMIS, explained in Ch. 2.6.2, should be triggered in this case, so that the information exchange between them is not compromised. The DE-SMIS send all their public data to their adjacent DE-SMIS and an aggregate analysis at DE-SMIS level is possible.

If a DE-SMIS is under (D)DoS attack, it red-flags itself to clarify to other DE-SMIS instances that they should avoid sending data. Only the communication path with the E-SMIS is preserved and the data exchange with it may become feasible. The DE-SMIS is able to receive indirectly through the E-SMIS information and threat patterns of their adjacent DE-SMIS instances.

14.3 Related Infrastructure

Breakout gateway, DSOSMC, DE-SMIS.

15. Threat and Countermeasure Mapping

Deliverable 1.1 [1] contains the identified threats to the system, particularly in Tables 2-1, 2-2 and Ch. 4.4 of D1.1. The following table indicates how those threats are mapped to the identified incidents and their countermeasures There is some overlap, so all entries from the identified parts of D1.1 are not included in the table). Green means the threat is covered by the countermeasure, orange that the threat is partially covered while red indicates that it is not.

Table 2: Threat to countermeasure mapping

Threat	I-1	I-2	I-3	I-4	I-5	I-6	I-7	I-8	I-9	I-10	I-11	I-N
Man-in-the-Middle												
Eavesdropping												
Masquerade												
Network Impersonation												
User Impersonation												
Wireless Network Threats												
Traffic Analysis												
Replay Attacks												
Virus / Worms												
Malware												
Trojan Horse												
Trapdoor												
SQL Injection												
Cross-site Scripting (XSS)												
MAC Spoofing												
Smurf Attack												
TCP sequence prediction												
Service Spoofing												
Denial of Service (DoS)												
Advanced Persistent Threats (APTs)												
Bypassing Controls												
Electromagnetic Radiation												
EM / RF Interception												
Jamming												
Data Injection Attacks												
Time synchronisation attacks												
Physical Threats/Intrusion												
Physical Theft												

16. References

1. success D1.1 V1.0, “Identification of Existing Threats, V1”, October 2016
2. success D4.1 v1.0, “Solution Architecture and Solution Description, V1”, July 2016
3. success D3.4 v1.0, “Information Security Management Components and Documentation, V1”, January 2017
4. Angioni, Andrea, et al. "Coordinated voltage control in distribution grids with LTE based communication infrastructure”, Environment and Electrical Engineering (EEEIC), 2015 IEEE 15th International Conference on. IEEE, 2015.
5. Dahlman, Erik, Stefan Parkvall, and Johan Skold, “4G: LTE/LTE-advanced for mobile broadband”, Academic press, 2013.
6. Dohler, Mischa, and Takehiro Nakamura, “5G Mobile and Wireless Communications Technology”, Eds. Afif Osseiran, et al. Cambridge University Press, 2016.
7. Pau, Marco, et al. "Low voltage system state estimation based on smart metering infrastructure”, Applied Measurements for Power Systems (AMPS), 2016 IEEE International Workshop on. IEEE, 2016.
8. 3rd Generation Partnership Project “Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)” Release 13, 2016
9. OMA Lightweight M2M (LWM2M), http://www.openmobilealliance.org/wp/Overviews/lightweightm2m_overview.html
10. ECOSSIAN D1.2 V1.0,” Requirements Report “, March 2015, stored at http://ecossian.eu/downloads/D1.2-Requirements-PU-M09.pdf (accessed 20161223)
11. Teixeira, André, Dán, György, Sandberg, Henrik, Berthier, Robin, Bobba, Rakesh B. and Valdes, Alfonso, “Security of Smart Distribution Grids: Data Integrity Attacks on Integrated Volt/VAR Control and Countermeasures',' *in Proc. of American Control Conference (ACC), Jun. 2014*
12. Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker, and Jonathan Turner. 2008. OpenFlow: enabling innovation in campus networks. SIGCOMM Comput. Commun. Rev. 38, 2 (March 2008), 69-74. DOI=http://dx.doi.org/10.1145/1355734.1355746
13. Analysis of the Cyber Attack on the Ukrainian Power Grid, March 18, 2016, E-ISAC

17. List of Abbreviations

3GPP	3rd Generation Partnership Project, mobile communications standardisation body
4G	4th Generation mobile communications system
5G	5th Generation mobile communications system
BR-GW	Breakout Gateway
BSF	Bootstrapping Server Function
CA	Certificate Authority
DCS	Data Centric Security
DEMS	Decentralised Energy Management System
DoS	Denial of Service
DDoS	Distributed Denial of Service
DE-SMIS	Distributed instance of European Security Monitoring and Information System
DPI	Deep Packet Inspection
DSO	Distribution System Operator
DSOSMC	DSO Security Monitoring Centre
DTLS	Datagram Transport Layer Security
EAP	Extensible Authentication Protocol
eNodeB	Evolved Node B, communicates wirelessly with UE in EPC networks
ESMC	Pan-European Security Monitoring Centre
E-SMIS	Security Monitoring and Information System
EPC	Evolved Packet Core, core network of LTE system
E-UTRAN	Evolved Universal Terrestrial Radio Access Network, part of EPC network
FLISR	Fault Location, Isolation, and Service Restoration
FIWARE platform	Future Internet Ware, open source components, development environment,
GBA	Generic Bootstrapping Architecture
GE	Generic Enabler
HSS	Home Subscriber Service, part of EPC network
HV	High Voltage
KPI	Key Performance Indicator
LV	Low Voltage
LTE	Long Term Evolution (4th Generation mobile communications system)
M2M	Machine-to-Machine
MME	Mobility Management Entity, part of EPC network
MV	Medium Voltage
NAF	Network Application Function
NAN	Neighbourhood Area Network
NFV	Network Function Virtualisation
NORM	New-generation Open Real-time Smart Meter
P-GW	Packet Data Network Gateway, part of EPC network
PMU	Phasor Measurement Unit
PUF	Physically Unclonable Function
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Network
S-GW	Serving Gateway, part of EPC network
SON	Self Organizing Network
TLS	Transport Layer Security
TPM	Trusted Platform Module
TSO	Transmission System Operator
UE	User Equipment, handset in EPC network
UICC	Universal Integrated Circuit Card
UUID	Universally Unique Identifier
VM	Virtual Machine

A. Examples of Recent Cyber Security Attacks Events

A.1 Recent Cyber Security Attacks Events at TSO Level

A.1.1 The ICT systems of 50Hertz under cyber-attack

On 20 November 2015, the ICT systems of 50Hertz – one of the four German TSOs, the company that manages the transmission of 40% of Germany's generated wind power – were been attacked.

Growing concerns about the vulnerability of Smart grids to digital assaults are not overstated at all. The cyber-attack suffered by 50Hertz, the TSO (Transmission System Operator) that is responsible for the operation of the transmission grid in Northern and Eastern Germany, confirmed it.

The onslaught, which was “serious but not dangerous" according to 50Hertz, lasted five days and came in the form of a DDoS attack (Distributed Denial of Service) against the company's internet domain, which resulted in the breakdown of the website and of the externally accessible services, such as the mail service. Attackers have not been identified, but the origins of IP addresses have been tracked down in Russia and Ukraine.

Although no transmission infrastructure and electricity supplies were affected by the assault, 50Hertz took it seriously and discussed it at a meeting of ENTSO-E (European Network of Transmission Systems Operators for Electricity).

The security of ICT systems working on power grids must be a priority for energy operators, according to a report recently produced by McAfee. Growing automation of power grids means higher vulnerability to cyber threats. In addition, the risks are higher for an old physical infrastructure.

For 50Hertz, that is the world’s leading renewable TSO (38% of the energy transmitted is produced by renewable sources), securing its system implies high investments, but the costs may prove prohibitive during a credit crunch. However, according to the CEO of ELIA (a Belgian company holding 40% of 50Hertz), ELIA have made huge investments in hardware so it would be a shame if ELIA’s system has been attacked through the proper software.

A.2 Recent Cyber Security Attacks Events at DSO Level

It is clear that Cyber Security Attacks are not only a possible threat, but they have been already proved to be possible. At DSO level, the most recent such event is the Ukraine cyber-attack which took place on 23rd of December 2015, where at least two DSOs have been hacked at dispatch level and a number of more than 200,000 people have been disconnected from the distribution grid by malicious commands in substations of the power grid. According to [13], seven 110 kV and twenty-three 35 kV substations were disconnected for three hours. In the document, it is said that “the attackers demonstrated a variety of capabilities, including spear phishing emails, variants of the BlackEnergy 3 malware, and the manipulation of Microsoft Office documents that contained the malware to gain a foothold into the Information Technology (IT) networks of the electricity companies”.

success is addressing methods for monitoring power and communication network activities in order to recognize abnormal behaviour and to be able to provide alerts which may reduce the impact of potential cyber-attacks.

The monitoring activity is based on key information extracted from NORM, containing power network related data with possible relevance from the network security point of view, or communication network data such as traffic patterns, which might reveal e.g. cyber-attacks. The data to be used by the monitoring centre need to preserve the privacy of end users, thus the

category of private data will be carefully addressed according with national and European relevant laws.

Moreover, the communication between the NORM Security Agent and the upper level (e.g. DSO Security Monitoring Centre) is established by using a more secure encryption method, based on Physically Unclonable Function (PUF), thus allowing a more trusted environment for the cyber-security aspects.

B. Overview of LTE

Figure 13 shows the current latest cellular network technology (LTE) that can be utilised for M2M type communications, in our case smart grid communication (for example wide area monitoring and control). LTE is the 4th generation of mobile communication technology and has been standardised by 3rd Generation partnership project (3GPP) community. Initial standards were specified in release 8, aiming to meet the demands of data traffic over mobile communication networks.

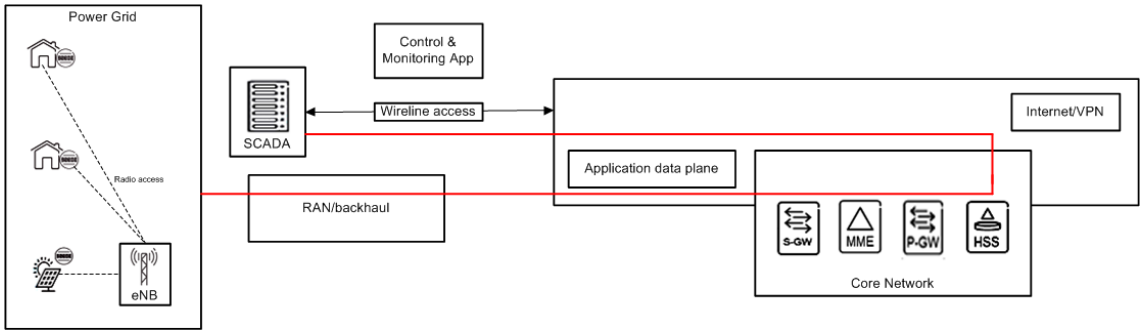

Figure 13: LTE for Smart Grid Communication

Mobile communication networks compromise two major components, the core network and the radio access network.

The **Radio network** consists of the Evolved Universal Terrestrial Radio Access Network (E-UTRAN) and User Equipment (UE), which is a device which provide authentication of end users. E-UTRAN is the air interface part of the LTE network. It consists of the eNodeBs (base stations) which provide radio related functions. These functions include radio resource management, scheduling, QoS, ciphering/deciphering of the user plane and control plane data and compression and decompression of the user plane packet headers [5].

The core network enables authentication, mobility, and connection to other non-3GPP networks. In LTE, the core network is known as the Evolved Packet Core (EPC) and it includes the following components.

The Mobility Management Entity (MME): The MME is the key control-node for the LTE access-network controlling the high-level operations such as authentication by means of signalling messages. It is responsible for user authentication and for regulating security parameters. It is also involved in the bearer activation/deactivation process.

Serving Gateway (S-GW): The S-GW routes and forwards user data packets. It is the node that terminates the interface towards E-UTRAN and acts as the mobility anchor for the user plane during inter-eNodeB handovers and for is responsible for compatibility between LTE and other 3GPP technologies

Packet Data Network Gateway (P-GW): The P-GW provides connectivity to the UE to external Packet Data Networks (PDNs) using the SGi interface. The UE may be simultaneously connected with more than one P-GWs for accessing multiple PDNs. This has two slightly different implementations, namely S5 if the two devices are in the same network, and S8 if they are in different networks.

Home Subscriber Service (HSS): It is centralised databased containing the information about all the mobile subscriber in the network. MME interacts with HSS to authenticate all the 3GPP device in the network.