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**: July 31 2016

**Actual Delivery Date**: July 29 2016

**Contributors**: LMF, RWTH, EDD, P3E

**Workpackage**: WP4 – Securing Smart Infrastructure

**Estimated person months**: (resources spent on the deliverable)

**Security**: PU = Public

**Nature**: R = Report

**Version**: 1.0

**Total number of pages**: 33

**Abstract**: The SUCCESS project is developing a new approach to the security of energy systems, guaranteeing their security of operation. This preliminary report describes the SUCCESS Architecture, the SUCCESS Security Management Solution and the SUCCESS Communication Solution.

**Keyword list**: Security, communication, Utility, Architecture

**Disclaimer**: All information provided reflects the status of the SUCCESS project at the time of writing and may be subject to change.
Executive Summary

Living in a safe and secure society is a fundamental human need. The security of critical infrastructures must be maintained so that supplies of power, water or other resources are secured. Modern critical infrastructures are increasingly complex and they are turning into Cyber-Physical Infrastructures because ICT is growing in importance in infrastructure management.

The SUCCESS project will develop an overarching approach to threat and countermeasure analysis with special focus on the vulnerabilities introduced by Smart Meters. The main challenge is to create the conditions in Europe for the future energy system to be as reliable as today.

Starting from a security by design approach and placing resiliency and survivability in focus, a new joint design of Energy Infrastructure and ICT is proposed.

Work Package 4 of SUCCESS will design the architecture of the SUCCESS system, including solutions for Security Monitoring and Communications. This preliminary report is the first of three reports on these topics.

The SUCCESS Architecture is developed based on an analysis of what features are expected to be supported in short-, medium- and long-term timescales. The Architecture is described from the viewpoints of Utilities, Security and Communications.
Document History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>Comment</th>
<th>Author/Editor</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.06.2016</td>
<td>V0.07</td>
<td>First draft</td>
<td>Padraic McKeever</td>
<td>RWTH</td>
</tr>
<tr>
<td>05.07.2016</td>
<td>V0.11</td>
<td>Ready for Review</td>
<td>Padraic McKeever</td>
<td>RWTH</td>
</tr>
<tr>
<td>07.07.2016</td>
<td>V0.12</td>
<td>2nd version for Review</td>
<td>Padraic McKeever</td>
<td>RWTH</td>
</tr>
<tr>
<td>20.07.2016</td>
<td>V0.13</td>
<td>Comments from 2nd review addressed</td>
<td>Gianluca Lipari</td>
<td>RWTH</td>
</tr>
<tr>
<td>28.07.2016</td>
<td>V1.0</td>
<td>Final version for submission</td>
<td>Gianluca Lipari</td>
<td>RWTH</td>
</tr>
</tbody>
</table>

Authors

<table>
<thead>
<tr>
<th>Partner</th>
<th>Name</th>
<th>e-mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>OY L M Ericsson AB (LMF)</td>
<td>Patrik Salmela</td>
<td><a href="mailto:patrik.salmela@ericsson.com">patrik.salmela@ericsson.com</a></td>
</tr>
<tr>
<td></td>
<td>Mohit Sethi</td>
<td><a href="mailto:mohit.m.sethi@ericsson.com">mohit.m.sethi@ericsson.com</a></td>
</tr>
<tr>
<td></td>
<td>Kristian Slavov</td>
<td><a href="mailto:kristian.slavov@ericsson.com">kristian.slavov@ericsson.com</a></td>
</tr>
<tr>
<td>RWTH Aachen University (RWTH)</td>
<td>Padraic McKeever</td>
<td><a href="mailto:pmckeever@eonerc.rwth-aachen.de">pmckeever@eonerc.rwth-aachen.de</a></td>
</tr>
<tr>
<td></td>
<td>Gianluca Lipari</td>
<td><a href="mailto:glipari@eonerc.rwth-aachen.de">glipari@eonerc.rwth-aachen.de</a></td>
</tr>
<tr>
<td>Ericsson GmbH (EDD)</td>
<td>Dhruvin Patel</td>
<td><a href="mailto:dhruvin.patel@ericsson.com">dhruvin.patel@ericsson.com</a></td>
</tr>
<tr>
<td></td>
<td>Syed Zain Raza Mehdi</td>
<td><a href="mailto:syed.zain.raza.mehdi@ericsson.com">syed.zain.raza.mehdi@ericsson.com</a></td>
</tr>
<tr>
<td></td>
<td>Frank Sell</td>
<td><a href="mailto:frank.sell@ericsson.com">frank.sell@ericsson.com</a></td>
</tr>
<tr>
<td>P3 Energy &amp; Storage GmbH (P3E)</td>
<td>Manuel Allhoff</td>
<td><a href="mailto:Manuel.Allhoff@p3-group.com">Manuel.Allhoff@p3-group.com</a></td>
</tr>
</tbody>
</table>
# Table of Contents

1. **Introduction** ................................................................. 6  
   1.1 Identifying information ............................................... 6  
   1.2 Supplementary information ........................................... 6  
   1.3 Overview ........................................................................ 6  
      1.3.1 Features Expected in the Different Timescales ................. 7  
         1.3.1.1 Medium Term (2020+) ......................................... 7  
         1.3.1.2 Long term (2030+) ........................................... 8  
   1.4 Concepts ....................................................................... 9  
      1.4.1 Security Concepts .................................................... 9  
      1.4.2 Utility Concepts .................................................... 9  
      1.4.3 Communication Concepts ....................................... 10  
         1.4.3.1 Long Term Evolution (LTE) .................................. 10  
         1.4.3.2 Network Function Virtualisation (NFV) .................. 10  
         1.4.3.3 Network Slicing ............................................... 10  
         1.4.3.4 Control Servers ............................................... 10  
   1.5 Other Information .......................................................... 10  
      1.5.1 Architecture Evaluations .......................................... 10  
      1.5.2 Rationale for Key Decisions ......................................... 10  

2. **Stakeholders and Concerns** ............................................ 11  
   2.1 Stakeholders ............................................................... 11  
   2.2 Concerns ...................................................................... 11  
   2.3 Concern–Stakeholder Traceability .................................... 12  

3. **SUCCESS Architecture: Utility Viewpoint** .......................... 12  
   3.1 Overview ...................................................................... 12  
   3.2 Concerns and stakeholders .............................................. 12  
      3.2.1 Concerns ............................................................... 12  
      3.2.2 Stakeholders ........................................................ 12  
   3.3 Block Diagram ............................................................... 12  
      3.3.1 Block Diagram Conventions ................................... 12  
   3.4 Operations on Views ....................................................... 12  
   3.5 Correspondence Rules .................................................... 12  

4. **SUCCESS Architecture: Communication Viewpoint** ............. 13  
   4.1 Overview ...................................................................... 13  
   4.2 Concerns and stakeholders .............................................. 13  
      4.2.1 Concerns ............................................................... 13  
      4.2.2 Stakeholders ........................................................ 13  
   4.3 Block Diagram ............................................................... 13  
   4.4 Operations on Views ....................................................... 13  
   4.5 Correspondence Rules .................................................... 13  

5. **SUCCESS Architecture: Security Viewpoint** ....................... 13  
   5.1 Overview ...................................................................... 13  
   5.2 Concerns and stakeholders .............................................. 13  
      5.2.1 Concerns ............................................................... 13  
      5.2.2 Stakeholders ........................................................ 13  
   5.3 Block Diagram ............................................................... 15  
      5.3.1 Block Diagram Conventions ................................... 15  
   5.4 Operations on Views ....................................................... 15  
   5.5 Correspondence Rules .................................................... 15  

6. **SUCCESS Architecture: Utility View** .................................. 15  
   6.1 View: Utility ................................................................. 15
6.1.1 Utility Conceptual Model: Timescale Today ........................................... 15
6.1.2 Utility Conceptual Model: Timescale 2020+ and 2030+ ........................ 16
6.1.3 Utility Topological Model Timescale 2020+ and 2030+ .......................... 18
6.1.4 Known Issues with View ................................................................. 19

7. SUCCESS Architecture: Communication View ........................................ 19
   7.1 View: Communication ........................................................................ 19
   7.1.1 Communication Conceptual Model................................................. 20
   7.1.2 Communication Topological Model ............................................... 20

8. SUCCESS Architecture: Security View ................................................... 22
   8.1 View: Security ................................................................................... 22
   8.1.1 Security Conceptual Model ........................................................... 22
   8.1.2 Security Topological Model ........................................................... 22
   8.1.3 Security Conceptual Model Timescale 2020+ and 2030+ ............... 23

9. Consistency and Correspondences ......................................................... 24
   9.1 Known Inconsistencies ..................................................................... 24
   9.2 Correspondences in the AD .............................................................. 24
   9.3 Correspondence Rules ..................................................................... 24

10. SUCCESS Security Solution ................................................................. 24
    10.1 E-SMIS ......................................................................................... 24
    10.1.1 Introduction ............................................................................... 24
    10.1.2 Previous Work ........................................................................... 25
    10.1.3 Architecture ............................................................................... 25
    10.1.4 Data Sources ............................................................................. 26
    10.1.5 ISMB specific study ................................................................. 27
    10.1.6 ENG specific study ................................................................. 28
    10.1.7 P3com specific study .............................................................. 28

11. SUCCESS Communication Solution .................................................. 28
    11.1 5G Key Enablers ......................................................................... 29
    11.1.1 5G Radio Access .................................................................... 29
    11.1.2 Network Function Virtualisation ............................................... 29
    11.1.3 Network Slicing ....................................................................... 29
    11.1.4 Devices .................................................................................... 29
    11.2 Why 5G for SUCCESS? ............................................................... 30
    11.3 Massive and Critical MTC ......................................................... 31
    11.4 SUCCESS Communication Solution: Timescale Now, 2020 – 2030 .... 31

12. References .......................................................................................... 32

13. List of Abbreviations ........................................................................ 33
1. Introduction

This document contains descriptions of:
- the SUCCESS Architecture, output of Task 4.2, which is described in Chs. 2-9 according to the ISO/IEC/IEEE 42010 standard [1].
- the SUCCESS Security Solution (output of Task 4.3) in Ch. 10, and
- the SUCCESS Communications Solution (output of Task 4.4) in Ch. 11.

This is the first, preliminary, version of the document. Two further updated versions will be produced in the course of the project.

1.1 Identifying information

This document describes the SUCCESS architecture.

It is an architecture description of the SUCCESS Platform system produced by Task 4.5 in the SUCCESS project for the SUCCESS field trials.

1.2 Supplementary information

This version of the architecture definition is intended to give a first definition of the needed functions, involved actors and technologies. For this reason, some paragraphs of this document are intentionally left blank, because these are the foreseen topics that need to be addressed and investigated in the next versions of this document.

1.3 Overview

The SUCCESS project’s work addresses three different timescales:

The timescales to be used are:
- Short Term: Investigations and results applicable to today’s Smart Grid Networks (2016)
- Medium Term: Investigations and results applicable to Next Generation Smart Grid Networks (2020+)
- Long term: Investigations and results applicable to Future Smart Grid Networks (2030+)

Based on a Threat Analysis, countermeasures are identified, implemented and trialled for the short, medium and long term. New long-term concepts for security, resilience and survivability of future Smart Grid Networks are developed.

![Figure 1: SUCCESS Time Horizons](image)

The timescales are reflected in the SUCCESS Architecture presented in this document. This version of the document is a preliminary version, released in project month 3 before the results of the Threat Analysis (WP1) and the security, resilience and survivability work (WP2) are
available. These results will be included in an updated version of this document to be released in project month 12.

Figure 2: SUCCESS Architecture Overview

The SUCCESS architecture, as shown in Figure 2, encompasses:

- components which provide security functionality from the meter or smart device at a range of levels right up to the pan-European Security Monitoring Centre level;
- communications based on mobile 4G and 5G technologies, including low latency;
- service APIs provided by a cloud-based middleware platform which interworks with devices and gateways in Utility’s grids;
- security applications, such as the European-level Security Monitoring Centre, which use these service APIs;
- New-generation Open Real-time Smart Meter (NORM)

Hence, the SUCCESS architecture covers both the different short-term, medium-term and long-term timescales and also the different aspects shown in Figure 2. In order to describe it in an ordered way, this document addresses the SUCCESS architecture by means of describing different views which address the different aspects. Separate Utility, Communication and Security views are given in Chs. 6, 7 and 8 below.

1.3.1 Features Expected in the Different Timescales

The features expected in the medium- and long-term are listed here.

1.3.1.1 Medium Term (2020+)

Power Grid:

- Real time Smart Meters (SM)
- Increase in penetration of Renewables
- Increased deployment of Storage systems
• more sensors in Distributed Generation (DG) to ensure voltage stability
• More grid automation to MV/LV
• more Automatic Fault Detection
• Advanced energy management systems
• Flexible tariffs (US already offering hourly prices in 2016)
• Demand response solutions
• Growth in energy services market
• Shift to platform based services offered in cloud, remote from energy provider (security monitoring centre)
• In Germany no nuclear by 2022, but more nuclear in other countries
• Increase in Electric Vehicles
• Cyber Security requirements increase, SCADA system requirements is a hot topic
• Security of supply concerns increase as renewables increase
• Smart Meter deployment is different in the different countries.
• More energy management, Smart Meters will not be stand-alone but integrated with Smart Home, Smart management, EM systems.
• Flexible tariffs: still early stages, not by 2020, but in US they have hourly pricing for the last 5 years. First movers in Germany will have this by 2020, others earlier. Services increasing already. Demand response will increase, trend towards offering services rather than products (e.g. offer and maintain PV panels).

Communication Technologies:
• Narrowband IoT communication.
• LTE with very big cells, devices can be reached in areas without voice coverage because voice needs 20dB more power in signal
• 5G communications (1st deployment)
• Software-Defined Networking (SDN)
• Network Functions Virtualisation (NFV)
• Low cost LTE IoT modems (long battery life, limited throughput, latency 200ms with optimisation, limited throughput, small (in watch), <10€) mass market in 2017)
• Cyber security requirements increasing.

1.3.1.2 Long term (2030+)
Power Grid:
• Microgrids planned as recovery from blackouts
• Microgrids as neighbourhoods power networks (peer to peer)
• Cyber security a major issue
• Privacy related concerns
• Renewables penetration >75%
• Energy as a Service will be major market force, e.g. rent heating system (owned by energy provider), and buy energy (kWh per year).
• Evolution in market structure (integrated supply of Gas, power, internet)
• Power grid architecture change (real time control and automation to LV level, distributed control, more meshed networks, more interconnects in EU, more cloud based control systems)
• Oil will be less relevant
• EV penetration >25% (>50%?)
• Integrated cross sector optimisation (transport, power, energy)
• Better generation and consumption forecasting, essential for power grid stability
• LV network architecture evolving, EVs and also storage systems in houses
• Germany will still be in transit towards renewables, e.g. it is building gas turbines now, reserve of power plants in system will still be in place (reserve inertia)
• Regulatory changes (pay for power and not energy)
• Services sold together with free goods (free USB sticks)
• User expectations (acceptance of technologies)
• Sharing economy
• Security problems
Communication Technologies:
- 5G communications widespread deployment
- Network Slicing available
- Breakout Boxes enabling microgrids recovery from blackouts
- Double Virtualisation available as solution
- Security improved to an extent that the currently known threats are mitigated by defining a new Architecture which is deployed by 2030 (SUCCESS ambition, possible scenario)
- Updates quick and automatic for new threats (from several weeks now down to one hour in 2030)
- Distribution of Precision Time Protocol for synchronisation of devices (e.g. low cost PMUs)
- More sophisticated attacks and detection systems
- Who wins the race? The battleground moves to new levels
- Standard security commonplace in energy and built into budgets
- Attacks organised increasingly on a large scale rather than individual hackers
- New disruptive technologies, currently not on our radars, will appear that will introduce new threats.

1.4 Concepts

1.4.1 Security Concepts

Security is the degree of resistance to, or protection from, harm. As with any communication system, the three high-level security objectives in Smart Grids are:

- Availability: Ensuring timely and reliable access to and use of information. This is important because a loss of availability is the disruption of access to or use of information, which may further undermine the power delivery.
- Integrity: Guarding against improper information modification or destruction is to ensure information non-repudiation and authenticity. A loss of integrity is the unauthorised modification or destruction of information that can further induce incorrect decision regarding power management.
- Confidentiality: Preserving authorised restrictions on information access and disclosure is mainly to protect personal privacy and proprietary information. This is in particular necessary to prevent unauthorised disclosure of information.

To ensure security, one has to rely on cryptography. Cryptography is the practice and study of techniques for ensuring secure communication in the presence of third parties called adversaries. In cryptography, encryption refers to the process by which messages or information is encoded in such a way that only authorised entities can decipher it. A digital signature on the other hand is used for demonstrating the authenticity of a digital message.

Symmetric-key algorithms are cryptographic algorithms for encryption that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. Public-key cryptography, or asymmetric cryptography on the other hand is a cryptographic system that uses a pair of keys: public keys that may be distributed widely, and private keys which are known only to the owner. With asymmetric keys, there are two functions that can be achieved: using a public key to authenticate that a message originated with a holder of the corresponding private key; or encrypting a message with a public key to ensure that only the holder of the corresponding private key can decrypt it.

1.4.2 Utility Concepts

Electrical grids are traditionally divided into three parts: generation, transmission and distribution. The traditional energy flow is from large, centralised Generation plants, over long distances through High Voltage Transmission lines to the Medium- and Low-Voltage Distribution Grid, where the end-consumers are reached. With increasing penetration of Distributed
Renewable Energy sources, however, significant amounts of energy are being generated in decentralised, small plants and fed into the Distribution Grid directly at MV- and LV- levels. Vertical integration is an arrangement in which the supply chain of a company is owned by that company. Contrary to horizontal integration, which is a consolidation of many firms that handle the same part of the production process, vertical integration is typified by one firm engaged in different parts of production.

A prosumer is a person who both consumes and produces electrical power. It is derived from "prosumption", a dot-com era business term meaning "production by consumers".

REST Services are web services where a simple, restricted set of actions may be used to access resources via their Uniform Resource Identifier (URI).

### 1.4.3 Communication Concepts

#### 1.4.3.1 Long Term Evolution (LTE)

LTE is a 3GPP release 8, network standard for mobile communication. It is also called 4th generation mobile communication technology. The current mobile network technology in use by mobile networks is LTE. LTE is further enhanced for supporting machine centric communication. These feature enhancements include narrow-band IoT, which is standardised by 3GPP to improve indoor coverage and better battery life, LTE low cost devices which are standardised in release 12, adapted for machine type communication. According to 2015 mobility report from Ericsson, LTE has already reached more than 1 billion subscriptions and the estimated number of users by 2021 is 4.3 billion. 90% of the Western Europe mobile traffic will be for LTE/5G by 2021 [26].

#### 1.4.3.2 Network Function Virtualisation (NFV)

NFV is a simple concept of network architecture. It virtualises the entire network and network nodes. NFV supports all the network functions and services that are being carried out by network hardware nodes. It runs on top of the hypervisor, requires a dedicated hardware just like x86 server. For NFV to become really useful, SDN technology is required. This allows management of network services by hiding physical deployments and presenting them as virtualized services.

#### 1.4.3.3 Network Slicing

Network slices concept in 5G is not a new one, VPN is a very basic version of a network slice. The networks will be further abstracted in to network slices, services defined by customizable software-defined functions that govern geographical coverage area, duration, capacity, speed, latency, robustness, security and availability [25].

#### 1.4.3.4 Control Servers

Control servers as shown in Figure 8 are the applications, e.g.; SCADA systems that are connected to the mobile network over the internet. So, the control servers can connect to the edge devices connected via mobile network. These control servers are basically the applications, monitoring devices in utility network.

### 1.5 Other Information

#### 1.5.1 Architecture Evaluations

- 

#### 1.5.2 Rationale for Key Decisions

-
2. Stakeholders and Concerns

2.1 Stakeholders

The stakeholders include a multitude of entities. From a security perspective, the entities include the customers, whose usage data and any personally identifiable information must remain private and secure. The user must also have access to high-quality service and should have sufficient energy supply to meet his/her demands. The user should also be protected from malicious billing. Since typically users are naïve when it comes to following security instructions, it is also important that any user actions required by the system are easy to perform and have low cognitive overhead. Similarly, another important entity from a security perspective is the utility company. The utility company wants to provide a reliable service to its customers and ensure that there are no free-riders or other malicious entities that circumvent the billing system.

As with any other network, the Smart Grid system would consist of devices and components from various manufacturers and vendors. It is important for a reliable service delivery and network performance that the devices and components perform reliably and contain no-known backdoors.

Other stakeholders include:
- SUCCESS project members
- SUCCESS Trial Sites
- Public users
- Users after SUCCESS project?
- Network operators providing cloud-enabled services to support power grid
- Energy retailers
- 3rd parties providing energy services

2.2 Concerns

Here we need to describe each Concern, or area of interest. The following questions express the concerns.

- What are the purpose(s) of the SUCCESS Platform?
- What is the suitability of the architecture for achieving the SUCCESS Platform’s purpose(s)?
- How feasible is it to construct and deploy the SUCCESS Platform?
- What are the potential risks and impacts of the SUCCESS Platform to its stakeholders throughout its life cycle?
- How is the SUCCESS Platform to be maintained and evolved?
- What are the dependencies between the different parts of the SUCCESS Platform?

From a security perspective, the SUCCESS Platform should take into account the entire lifecycle when designing the security components. The lifecycle for any component would start with the initial manufacturing and deployment phase, span through the operational phase, and continue until the recycling or decommissioning of the concerned component.

While the exact components used for the SUCCESS Platform would change over time as the platform itself evolves based on the feedback and experiences from the trials, we intend to rely on well-studied and evaluated security protocols and suites. The use of standardised protocols would also enable easy integration with the rest of the system components and provide interoperability.

As noted by Bruce Schneier, it is also critical to ensure that the platform has adequate secure remote-update capabilities. This is because, over time, new vulnerabilities and security issues would be discovered and therefore it should be possible for utility companies and smart meter vendors to update and patch any vulnerabilities that are found.

From the Utility point-of-view, the SUCCESS Platform should enable interoperability between devices in different grids and services based on the data generated by the devices, enabling a move from vertically-integrated Utilities to having services offered by different specialised companies. The SUCCESS Platform should offer secure, reliable, cost-effective
communications to very large numbers of devices based on open and standardised interfaces and off-the-shelf technologies.

2.3 Concern–Stakeholder Traceability
Will be added in later version.

3. SUCCESS Architecture: Utility Viewpoint

3.1 Overview
The viewpoint covers Utility grids, such as the electricity, gas or water grid and grid-specific equipment and systems. It includes the components in the grids, the functions performed by them and the information passed between them.

This viewpoint excludes communication between grid components and security, which are covered by other viewpoints.

3.2 Concerns and stakeholders

3.2.1 Concerns
- Maintaining grid stability while enabling increasing amount of DERs to be introduced into the distribution grid.
- Coping with the change from having power generated overwhelmingly by large conventional power plants feeding into the HV network to having most of the power generated by DERs and feeding into the MV and LV networks.
- Increasing level of monitoring and automation of DGs;
- Enabling new and innovative Energy Services to be offered to energy customers.
- Enabling DSOs to avail of cost-effective, standardised and modern ICT technologies;
- Enabling new business models to emerge and new actors to enter the energy domain.
- Enabling change having vertically integrated Utilities in DGs to separation of ownership of generation, grid operation, grid services and customer services.

3.2.2 Stakeholders
- DSOs
- Prosumers
- ICT companies
- Cloud infrastructure providers
- Energy Service providers
- Energy markets
- Energy aggregators

3.3 Block Diagram

3.3.1 Block Diagram Conventions
Block diagrams are drawn using basing on FMC http://www.fmc-modeling.org/. In particular, the TAM Visio stencils are used.

3.4 Operations on Views
Will be added in later issue.

3.5 Correspondence Rules
Will be added in later issue.
4. SUCCESS Architecture: Communication Viewpoint

4.1 Overview
This viewpoint covers the communication for utility grids.

4.2 Concerns and stakeholders

4.2.1 Concerns
From communication perspective, the most important concerns are following:
- Latency: Latency is the time it takes to travel from source A to destination B.
- QoS: It is the performance of communication channel. In communication network, QoS parameters are defined.
- Coverage: Coverage is the geographical area covered by the radio station. Here the main concern is indoor penetration since in smart grid network, utility meters are installed inside homes and in cellars so indoor network coverage is very important.
- Power consumption of the devices: Smart grid communication gateways must be less power consuming in order to have more battery life and less maintenance cost.
- Bandwidth: Bandwidth is the amount of data that can be transferred in some particular time limit.

4.2.2 Stakeholders
The stakeholders of the communication viewpoint are the Telco service providers, Telco manufacturers and utility grids.

4.3 Block Diagram
Will be added in later issue.

4.4 Operations on Views
Will be added in later issue.

4.5 Correspondence Rules
Will be added in later issue.

5. SUCCESS Architecture: Security Viewpoint

5.1 Overview
The viewpoint covers security for utility grids, such as the electricity, gas or water grid and grid-specific equipment and systems.

5.2 Concerns and stakeholders

5.2.1 Concerns
For distribution automation, availability, integrity and authenticity are critical, while confidentiality has less importance [1]. To this, the following additional security objectives can be added:

- Authenticity: Ensuring that devices can mutually authenticate each other through the use of shared secrets. [3]
- Authorization: Concerned with ensuring access to system functions (e.g. via API) is obtained only by actors with proper permissions.
- Auditability: Being able to reconstruct a history of events from records of actions taken on the system.
Security is needed at all the different layers of the network and device stack. Here we elaborate the security requirements and solutions at different layers:

- **Application layer security**: The North American Electric Reliability Corporation (NERC) has defined a series of requirements for protection of critical cyber assets. Part of the requirement is that electronic access controls and monitoring of electronic access shall be implemented to restrict access to authorised users and detect and alert for unauthorised access or attempted access [5]. Central Authentication, Authorization and Accounting (auditable) management (AAA) is important to prevent network access of unauthorised devices or users at the application level [6]. Authentication and authorization services must be able to operate in an autonomous manner at the local level to avoid lock-out if the communication link to the central authority is lost. Use of insecure protocols presents a further risk at the application layer [1]. RADIUS and Diameter are specific protocols commonly used for AAA security [3] [7] [8].

- **Transport layer security**: Transport layer security (TLS) protects data above the transport layer and is designed to prevent eavesdropping, tampering or message forgery [3]. Protocols such as TLS and IPSec provide secure end-to-end communications that ensure confidentiality and integrity of regardless of the intermediate hops [6]. The International Electrotechnical Commission (IEC) standard, IEC 62351, specifies the security requirements for data and communication security for power systems. TLS is specified for IEC 61850 protocols as detailed in IEC 62351 [14]. Therein, for example, substation communications are required to support the following cipher suite TLS_DH_RSA_WITH_AES_128_SHA [14].

- **Network layer security**: IPSec offers cryptographically-based security for IPv4 & IPv6 at the network layer to create a virtual private networks (VPN). It provides confidentiality (via encryption), access control, integrity, data origin authentication and detection and rejection of replays. Moreover, the IPSec security protocols (Authentication Header (AH) and Encapsulating Security Payload (ESP)) are designed to be independent of the cryptographic algorithm, which allows selection of different sets of algorithms as appropriate. Most security requirements can be met with ESP as it can be configured to provide integrity and data origin authentication without confidentiality [9]. This is noteworthy for smart grid applications, such as substation automation, where data confidentiality could be traded for reduced latency. By offering protection at the lower network layer the host can identify legitimate messages and discard others thereby reducing the vulnerability [3]. In other words, devices should not act on traffic that does not conform to the protocol or message standard [1].

- **An IPsec security association (SA) must be established between two end points via a key management protocol, for example the Internet Key Exchange (IKE) protocol [9]. Keys can be pre-shared (symmetric) or dynamically distributed (asymmetric) using Public Key Infrastructure (PKI). The advantage of symmetric keys is that it is computationally faster, while asymmetric keys allow for scalability and more efficient key management through automation of key generation and distribution [10] [15]. In the case of substation automation where IEDs transmit a broadcast message (filtered to multicast) then IPsec must support multicast SAs.

- **Link layer security**: It is stated by NERC [5] that Critical Cyber Assets shall reside within an Electronic Security Perimeter (EPS). For wireless technologies, eavesdropping is typically of a concern [3]. LTE counters this by providing mutual authentication based on the Universal Subscriber Identity Module (USIM), with integrity and replay protection and strong encryption (128 bit keys) of the signaling between the terminal and the Radio Base station (RBS). The transport between the RBS and the core network is protected by IKE/IPsec. Once the connection is established, the user-plane traffic between the RBS and the terminal is protected by strong encryption as integrity protection would result in too great an overhead [13]. Relying solely on the link layer protection of LTE is not sufficient for mission critical data and a defense in depth strategy must be considered.

- **Physical layer security**: Access to physical hardware offers vulnerability that could lead to compromise of the network. Physical access should be limited based on criticality of the device. Tamper resistance, tamper/intrusion detection and alerts can complement
physical barriers such as secure locked buildings [11]. With regard to physical security, NERC specifies that all Cyber Assets within a defined Electronic Security Perimeter shall sit within an identified Physical Security Perimeter. Physical access points and access control measures shall be identified and controlled through, for example, key cards. Monitoring and logging of physical access shall also be undertaken through, for example, video surveillance [12]. This should be applied in the context of electrical grid asset protection as specified in [5]. The use of physical unclonable function (PUF) is also needed to ensure physical security.

When utilizing 3GPP for network access, some security functions are already provided by the network; the device and network mutually authenticate, the control signaling is protected end-to-end and the user plane communication is (typically) protected on the air interface. In addition, the 3GPP credentials and infrastructure can also be used for authentication and key agreement for non-3GPP service through the use of the Generic Bootstrapping Architecture (GBA, 3GPP TS 33.220). After this, the established key material can be used for setting up network, transport or application layer security.

In addition to building a secure system it is also important to be prepared for a potential breach of that security. This can be done by implementing methods and tools for detecting, reacting and mitigating the attacks. One way of trying to contain an attack is to isolate the affected part of the system, possibly through the use of virtualization techniques, e.g. NFV and SDN, for reconfiguring the network.

5.2.2 Stakeholders

The main stakeholders are the utility companies who deploy their infrastructure and need it to be properly secured to provide reliable service and protection against possible attacks. Of course, this is closely related to the customers of the utility companies, who expect that their service is uninterrupted and that their possibly privacy sensitive information is handled with care and according to regulations. Also individual component providers need to make sure that the products they are providing meet the security requirements, also taking into account new discoveries related to possible security flaws in the products or protocols used.

5.3 Block Diagram

5.3.1 Block Diagram Conventions

Block diagrams are drawn using basing on FMC http://www.fmc-modeling.org/. In particular, the TAM Visio stencils are used.

5.4 Operations on Views

Will be added in next issue.

5.5 Correspondence Rules

Will be added in next issue.

6. SUCCESS Architecture: Utility View

6.1 View: Utility

The name of this view is Utility.

6.1.1 Utility Conceptual Model: Timescale Today
Today's Distribution Grids are characterised by vertical integration. Each DSO owns the physical grid, the devices in it and the management systems which control and manage it. This is illustrated in Figure 3 by showing two DSOs, A and B with exactly the same equipment.

The Devices in Figure 3 are any physical devices in the Distribution Grid which have sensors and/or actuators, i.e. devices which produce measurements or can be operated or controlled. There are many such devices, e.g. transformers, circuit breakers, Smart Meters, DERs, EVs, BMSs, EMSs.

The protocols towards the Devices are generally standardised, although proprietary protocols may be in use.

There is a number of different Management Systems performing different roles in the DSOs enterprise, such as managing the grid, customer care, billing. The interfaces between the Management Systems are partly standardised, partly proprietary, according to the particular DSO and the history of the development of their management infrastructure. It is unlikely that two DSOs will have the same Management Systems. It is also the case that the data generated in one DSO’s grid remains there and is not shared with any third parties.

The level of grid automation present in Distribution Grids today is limited. Generally, there is little or no measurement equipment beyond the secondary transformer, so that the DSOs do not have detailed information about the actual grid status. Any Smart Meters deployed are used for billing purposes only.

6.1.2 Utility Conceptual Model: Timescale 2020+ and 2030+

The shift energy services offered from cloud-based platforms and the growth in the energy services market is reflected in the conceptual model of Figure 4. It shows a cloud-based platform, called Utility Management Platform (UMP), which interworks with the devices in the Distribution Grid and acts as a gateway between the devices and grid management functions (called “Apps”, but in principle the same as (and including) today’s Distribution Grid Management Systems). The UMP gathers measurement data, processes it and making it available to the App. Then the UMP controls and actuates the devices in the grid based on the orders from the Apps. Such platform will be used as starting point for the development of the SUCCESS Architecture.

The salient difference to today’s Distribution Grids is the interoperability between Devices and Apps. The data from a given DSO’s Devices can be made available to third parties. Today’s vertical integration within the DSO is removed and the creation of new services, the entry of new players with specialised competences is made possible. This will both enable faster change in
the Distribution Grid management architecture and allow this change to be successfully introduced.

Platforms such as the UMP can use the services of other such Platforms and also interwork with existing Distribution Management Systems by means of publishing their offered services and using standardised interfaces.

Figure 4 shows a general conceptual view of the Utility Layer in SUCCESS. It covers both the 2020+ and 2030+ timescales, i.e. no conceptual architectural change in considered necessary to cope with the changes in the power grid in this period. It is a Service-oriented Architecture. In this view,

- devices represent grid equipment which produces data or can be managed; devices may be accessed directly by the UMP or through a gateway;
- the Apps are grid management applications which use services of the UMP to manage the grid;
- the UMP represents functionality which supports interoperability between devices and apps. It offers a set of services to the Apps.

Example of Devices: NORM, EVs, Smart Meters, PMUs, Smart Charger


![Conceptual Model of Utility Grid in 2020+ and 2030+](image)

**Figure 4: Conceptual Model of Utility Grid in 2020+ and 2030+**
The SUCCESS API defines a set of Utility services, offered as REST web services, continuing the approach of the FINESCE API developed by FINESCE.

The NORM Smart Meter Gateway is used to connect the Utility devices to the UMP. Real-time Smart Meters can use the NORM as a gateway which concentrates the measurements or, can communicate directly with the UMP, subject to communication requirements being met.

Alternatively, Utility devices may be connected directly to the UMP.

The UMP Middleware contains a data model for the SUCCESS domain, and performs data processing and storage.

The Device Adapters in the UMP interface between the protocols used between the Devices and the UMP and the UMP Middleware’s data model.

The Utility Services in UMP use the Middleware as basis for accessing the data needed and as provider of service building blocks.

The Utility Services and the data storage in UMP are virtualised, i.e. not directly associated with particular physical equipment:

- The Utility Services are implemented in a distributed cloud platform and accessed as resources through URIs. They are thus independent of any particular physical infrastructure.
- The UMP’s data storage is implemented in a distributed database in the distributed cloud platform and is thus independent of any particular physical infrastructure.

The UMP will be based on the platform produced in the FINESCE project, which uses general-purpose open-source components from the FIWARE program as building blocks. These components are referred to as Generic Enablers (GEs), and they are generic in the sense that their functionality can be applied in different domains, such as Medicine, Logistics, Smart Grids etc. The term Domain-specific Enabler (DSE) is also used in FIWARE and refers to open-source components whose functionality is specific to a particular domain. FINESCE developed a number of DSEs. SUCCESS UMP will base on FIWARE’s components and will adopt a policy of publishing any new components it develops as open-source (GEs or DSEs).

6.1.3 Utility Topological Model Timescale 2020+ and 2030+

This model gives more details on the types of Devices and Apps expected in the grid in the future, basing on the Conceptual Model of 6.1.2. The Devices in the Conceptual Utility View correspond to equipment in the Electricity Grid in the Utility Topological View.

The UMP is a cloud-based platform.

Different instantiations of the Platform can be introduced as needed, e.g. for different microgrids or different parts of grids in general. The use of cloud technologies offers the advantage of scalability, so that the increase in the amount of DERs, EVs, services, automation between the medium- and long-terms can be catered for.
6.1.4 Known Issues with View
Will be added in next issue.

7. SUCCESS Architecture: Communication View

7.1 View: Communication
The name of this view is Communication
7.1.1 Communication Conceptual Model

The general conceptual view of the communication architecture is shown in Figure 6. It consists of four layers.

- At the lowest level are the devices and gateways, which enable connectivity over wired or wireless medium. These devices gather data and transmit it to the upper layers. Connectivity enables the communication between the devices and the services. The type of connectivity could be wired or wireless supporting wide range of protocols.
- Service Enablement: It enables the services and provides the core functionality of the whole communication. such as enabling protocols, messages and configurations.
- Applications are the services which require the underlined data from the devices through connectivity and service enablement layer.

![Communication Conceptual Model Diagram](image)

Figure 6: Communication Conceptual Model

The communication architecture is independent of the use cases. This means that this architectural model can be used for many types of use cases. Use cases address the end-to-end capability of the communication architecture, implying that use cases affect all layers of the architecture.

When a specific use case is realised, relevant functions from each layer are deployed. For example, if a device or gateway makes use of 3GPP communication, it will locally use services available through the 3GPP modem and trigger corresponding network services. Examples for such network services can be functions for support of mobility or 3GPP authentication.

In an interaction between the connectivity and service enablement layers, relevant information is provided, for example how a service can reach a particular device or gateway. From the service enablement layer capabilities are exposed, so that applications can, for example, limit connectivity.

7.1.2 Communication Topological Model

All functions of the layers in the conceptual model can be mapped to the layers in the topological model. Some aspects of the mapping between conceptual and topological model are described further below.
The devices can be connected via gateways which aggregate communication from limited devices or directly when devices have own access capabilities, for example a 3GPP modem. In the access layer corresponding access technologies are supported so that radio or broadband access can be terminated in this layer and communication paths to the network and application services can be established. Applications are typically realised in control servers, but in some of the SUCCESS scenarios parts of the application functionality is executed in the break-out gateway (BR-GW). These break-out gateways are located close to the access points so that for example edge computing allows the reduction of network latency.
The 5G Core includes classic connectivity functions such as mobility services, but also enhanced service capabilities, which are relevant for connectivity services for IoT devices. An example is the handling of device addresses so that network initiated services can connect to the correct device, even if subscription details are not known to the controlling application.

8. SUCCESS Architecture: Security View

8.1 View: Security

The name of this view is Security.

8.1.1 Security Conceptual Model

The security model has security enablers on each layer mapped with Communication conceptual model, the security enablers are the functions which enables the security.

Network Access Control (NAC) enforces the policies that describe how the nodes will connect to the network. Physically Unclonable Function (PUF) is embodied in to the device that makes it harder to predict and practically impossible to duplicate, it is a type of cryptography. Connectivity layer security enablers, enables the encryption and ciphering over the wireless communication. It makes sure that the data which is transmitted over the connectivity layer is encrypted. Device authentication and authorization enables the authentication of correct device which connects to the network. Data Integrity refers to assuring the accuracy of the data over its entire life-cycle. On top of everything, a Pan European security architecture will be implemented. There could be multiple security enablers with multiple security functions in each enabler. The security function such as device authentication can also be enabled on devices.

![PAN European Security Architecture](image)

**Figure 9: Security Conceptual Model**

8.1.2 Security Topological Model

The layers in the conceptual model refer to the actual nodes and devices in the network, and the security functions implemented by them. The devices connect via the access network (connectivity) to the core network (connectivity and service enablement). The devices are mutually authenticated with the core network based on their credentials and the matching credentials stored in the core network in HLR/HSS or AAA server and will be used for security services such as authentication or encryption. In addition, the devices and services residing on the device might further authenticate to application services or other devices, possibly with
different credentials. The access network provides some communication security, while the devices use additional security protocols as needed for securing communication end-to-end. This can include e.g. transport layer security and application layer security.

8.1.3 Security Conceptual Model Timescale 2020+ and 2030+

The features expected in the medium- and long-term from a security point of view are discussed next.

Medium term (2020+): A majority of the ongoing security standardization work for 5G, IoT and Smart Grid security happens at the Internet Engineering Task Force (IETF), 3 Generation Partnership Project (3GPP) and Institute of Electrical and Electronics Engineers (IEEE). We expect that in the medium term, a lot of the standardised protocols will see increased field trials and deployment. Here we highlight the important ongoing work in these standardization bodies which will likely see larger deployment in the medium term:

In recent years, the IETF has worked on a new version of the HTTP protocol. The new version is called HTTP/2, and it provides performance improvements by means of a binary representation of the commands. Other improvements include header field compression and support of multiple exchanges on the same connection. HTTP/2, published as IETF RFC 7540 (May 2015). On the security side, the HTTP/2 RFC states that TLS version 1.2 or a higher version must be used for HTTP/2 over TLS. The new phase of work also focuses on opportunistic encryption for HTTP. This proposal makes it possible to run HTTP over TLS and encrypt the communication, without requiring strong server authentication (17 March 2016).

The IETF is also updating the TLS protocol (the latest draft is for TLS is v 1.3, 21 March 2016). One of the main goals of the new version is to encrypt as much as possible of the handshake messages to reduce the amount of data available to attackers. Another major goal is to reduce the handshake to one round-trip. TLS 1.3 will also update the profiles to address known weaknesses in CBC block cipher modes and RC4.

The Internet of Things (IoT) is one of the areas where IETF has been dedicating a considerable amount of effort. Whilst HTTP can be used for IoT devices, a new lighter weight version of the protocol has been defined for Constrained Devices. That protocol is called “The Constrained Application Protocol (CoAP)”, which is specified in RFC 7252. CoAP is based on the same Representational State Transfer (REST) architecture and provides a generic request/response interaction model similar to the Hypertext Transfer Protocol (HTTP). However, unlike HTTP, messages in CoAP are exchanged asynchronously over the unreliable datagram-oriented transport such as UDP with optional reliability.

Datagram Transport Layer Security (DTLS) provides communications privacy for datagram protocols and is based on the standard Transport Layer Security (TLS) protocol that is used widely on the Internet. The CoAP base specification provides a description of how DTLS can be used for securing CoAP. It proposes three different modes for using DTLS, namely: Preshared key mode (where nodes have pre-provisioned keys for initiating a DTLS session with another node), Raw Public Key mode (where nodes have an asymmetric-key pair(s) but no certificates to verify the ownership) and Certificate mode (where public keys are signed in certificates by a certification authority). In addition, IETF has also specified an implementation profile for TLS version 1.2 and DTLS version 1.2 that offers communications security for resource-constrained nodes that are part of IoT.

The CoAP specification also provides an alternative approach for securing communication with Internet Protocol Security (IPSec). It argues that many constrained devices already have support for link layer encryption in hardware which can be used to make IPSec a viable option in such networks. There is work ongoing in this area with the standardization of header compression for IPSec.

There are also other communication security issues associated with resource-constrained IoT devices that sleep during their lifecycle to save energy. Such IoT devices cannot afford to stay online for large amounts of time to be polled for data or support computationally intensive security protocols. To ensure data integrity, authenticity and confidentiality in such devices, the cryptographic protection measures need to be applied directly to the application-layer message objects. This method of communication security is also referred to as “object security”.

Page 23 (34)
Access control mechanisms are a necessary and crucial design element to any application’s security. Therefore, it is not surprising that IETF is also investigating how web-based access control and authorization solutions can be applied to resource-constrained devices that are part of the IoT. It is currently defining an authorization and access control framework for resource-constrained nodes based on the OAuth 2.0 framework, which is currently the de-facto standard for authorization on the web.

IEEE has recently initiated the formation of some projects related to privacy in IEEE protocols. Specifically, the creation of project “P802E - Recommended Practice for Privacy Considerations for IEEE 802 Technologies” which is intended to draw up recommendation documents on Privacy in IEEE 802. This group was formed as a result of an IEEE Project Authorization Request (PAR) from the IEEE 802 EC Privacy Recommendation Study Group. The IEEE privacy study group coordinated some MAC randomization trials at recent IETF meetings in Hawaii (IETF91), and Berlin (IETF92), and at one IEEE 802 standards meeting.

SA3, the 3GPP security group, with its new SI on Study on the Security Aspects of the Next Generation System (TR 33.899) will potentially result in many security enhancements for 5G which will also be deployed in the context of Smart Grids.

Long term (2030+): From a long term security view perspective, the most important development, beyond what is discussed for 2020+, we believe would be in field of quantum computing. As quantum computers become a reality, many of the well-known asymmetric, public-key algorithms such as RSA may need to be replaced or may require significantly longer key sizes to ensure security. This will also have impacts on the overall performance of the system.

9. Consistency and Correspondences

This chapter describes consistency requirements, recording of known inconsistencies in the Architecture Description, and the use and documentation of correspondences and correspondence rules.

9.1 Known Inconsistencies

Will be added in next issue.

9.2 Correspondences in the AD

Will be added in next issue.

9.3 Correspondence Rules

Will be added in next issue.

10. SUCCESS Security Solution

This chapter documents the result of Task 4.3, which includes defining the final architecture as well as its implementation.

10.1 E-SMIS

10.1.1 Introduction

Energy distribution networks are critical infrastructures covering large geographical areas requiring adequate protection mechanisms. Wide Area Monitoring Systems (WAMS) are essentially based on a new data acquisition technology that allows monitoring system conditions over large areas in view of detecting and further counteracting grid instabilities. The measured quantities are taken by ubiquitously distributed devices placed at selected locations in the power system and stored in a data concentrator approximately every 100 milliseconds. By comparing the snapshots with each other, the steady state and the dynamic state of critical nodes can be observed. Thereby, a dynamic monitoring of critical nodes in cyber-physical systems can be achieved. This kind of system can also be defined as an “early warning system” as it contributes
to an increase in the system reliability by avoiding the spreading of large area disturbances, and optimizing the use of assets.

We introduce the European Security Monitoring and Information System (E-SMIS) as a new approach to analyse various data sources and to identify threats associated with critical energy infrastructure. These threats can only be identified with a comprehensive view on several data sources across Europe. E-SMIS gathers information that is provided by DSOs and TSOs in Europe, evaluates the data with regard to common patterns, such as cyberattacks, and then shares these patterns with the DSOs and TSOs. Thereby, the DSOs and TSOs obtain information that cannot be derived from their local, non-European level. Their local level does not provide enough data for a correct classification of potential patterns. Additionally, E-SMIS takes into account further open data sources to strengthen the conclusion of the identified common patterns. E-SMIS evaluates and visualises various data characteristics in real time.

10.1.2 Previous Work

There is no tool available that systematically analyses data of energy related fields and that integrates the results with further open data sources. However, to visualise large amounts of data, we can resort to various well-known tools, such as scalyr [16], graylog [17], sumologic [18], logentries [19], loggy [20], openTSDB [21], FLUME [22] and ELK [23]. The majority of these tools are tailored for the analysis of log files in distributed computer networks. Moreover, Splunk is a proprietary, closed-source tool that visualises the data and that can also perform standard data analysis techniques. Tableau is a professional and flexible solution to display data.

In the past, energy metering data were used for billing purposes only. Wide Area Management Systems were assisted by different real time data sources such as the PMUs and RTUs. In the customer-centred energy distribution networks, real time energy meters start supplying very peculiar kind of data useful for decentralised grid optimization. This project uses the new generation meters (NORMs) and the low cost equivalents of phasors. These devices provide new data useful to protect the energy distribution system. Specifically, real time process oriented hybrid devices can supply precious data to the decision makers and to the e-SMIS.

10.1.3 Architecture

E-SMIS follows a multitier architecture comprising a data presentation, result management, data processing and data management tier shown in Figure 10:

- Tier 1: the data management tier stores the data E-SMIS is working with. The data comprise open and private data sources.
- Tier 2: the data processing tier implements all analysis steps necessary to identify common patterns in the data. This layer computes results E-SMIS depictions in Tier 4. Tier 2 is organised in separate modules where each module (1) receives data from Tier 1 (2) performs specific evaluation methods and (3) stores results in Tier 3. Step (1) and (3) are performed by interaction with Tier 3 and Tier 1, respectively. Step (2) resorts to various statistical and algorithmic strategies, such as correlation analysis, cluster algorithms, graph algorithms, hmm, gmm or neural networks. The aim of these methods is to derive common patterns from the data.
- Tier 3: the result management tier stores the results obtained from the data analysis in Tier 2.
- Tier 4: the data presentation tier presents information to the user. Data from different sources, which is computed by the result management tier (Tier 3), is integrated. That includes statistical analyses performed to identify irregularities in the data. There is no input from other tiers.

We distinguish within the data processing, result management and data management tier between public and private applications. Due to data privacy politics, DSOs and TSOs most likely do not give out their measured data. To model that condition, the data can therefore either stem from public or private sources (see Tier 1 in Figure 10). These data sources are not connected. As a consequence, the functional implementation in the data processing tier is also divided into a public and private application. The private application can be performed locally at the DSOs or TSOs, whereas the public data can be processed and provided in a centralised way. Consequently, the logic for the private data in the data processing tier can access to the open data as well as to the private data. In contrary, the logic for the open data can also only
obtain data from the open data sources (see Tier 1 in Figure 10). Thereby, we obtain a decentralised system architecture.

E-SMIS follows the idea of a plug-in strategy to be extensible for new analysis methods. To incorporate a new analysis method as a plug-in the following steps have to be performed: first, if necessary, new data is added to the data management tier (see Tier 1 in Figure 10). Second, the data management tier provides the data to an evaluation strategy module in the processing tier (see Tier 2 in Figure 1). The results are stored (see Tier 3 in Figure 10) and finally, the presentation tier (see Tier 4 in Figure 1) displays the information in a novel view.

10.1.4 Data Sources

We list potential data sources that we can use to identify common patterns in the data of the power system in a European-wide manner. Main data sources describe the core elements for the evaluation analysis. Data from DSOs and TSOs are potentially not publicly available. Main data sources are:

- threat and counter measurement repositories obtained from WP1 and WP3.
- real time energy data coming from NORM devices.
- low cost equivalents of phasors coming from newly extended NORM meters.

Additional data sources for the threat detection are open data. Open data can be integrated to strengthen the statement of the data analysis. Potential open data sources are:

- energy data: netzdaten-berlin.de offers 189 historical data sets. Moreover, the European Network of Transmission System Operators for Electricity (ENTSO-E) offers energy related open data. Both data sources can be used to train a model that serves as a gold standard in the downstream evaluation.
- simulated data: data based on energy grids can be simulated by real time digital simulators to obtain a ground truth for the system behaviour.
- weather data: plenty of providers offer historical, current as well as predictive data of the weather. A correlation to energy-related data is well-known.
- social network data: further data can stem from for example from Facebook, twitter or Instagram. We can evaluate a potential correlation between the social network and energy data.
- geographic data: Copernicus is a system developed by the EU that monitors the earth with satellites. Similar to the social network data, a potential correlation to the energy data can be evaluated.
In the decentralised customer-oriented grid management scenario, process-oriented measurement devices installed grid-wide supply the data to the Multi-Agent System running the collective optimization of the energy resources. It is a novel technology aimed to improve the energy efficiency and to increase the resilience of smart grids. The above mentioned real time measurement devices can supply relevant data to the E-SMIS. However, the flow of the data generated in real time is characterised by the high speed (V1) and high variability (V2). It represents a challenge for the E-SMIS system in terms of the data processing capabilities. In this case, the grid monitoring and analysis operations use the real time Big Stream Data processing.

10.1.5 ISMB specific study

In customer-centred networks, optimization of the renewable energy resources is implemented in decentralised manner. It implies very different schemes for the data distribution between decision-making agents. In the centralised approach, it was sufficient to deliver information to the control agent in order to empower it. In the decentralised approach, every agent should receive relevant information in order to actuate collective optimization decisions.

Data Stream Mining is the process of eliciting knowledge from high-speed data records. Data stream from NORM-like networked devices is an ordered sequence of instances that can be read only once or a small number of times using limited computing and storage capabilities. In this specific application, the goal is to predict the class or value of new instances in the data stream given some knowledge about the class membership or values of previous instances in the data stream.

Human-brain-like Intelligence, for example Machine learning techniques, can be used to learn this prediction task from labelled examples in an automated fashion. The required capability is to cope with structural changes inside the data stream due to the presence of fake data or altered devices. In SUCCESS application operating within non-stationary environment, the distribution underlying the instances or the rules underlying their labelling may change over time. For this reason the goal of the prediction, the class to be predicted, and the target value to be predicted, all out of them may change over time.

SUCCESS Security Management Solution (CSMS) will receive novel and sophisticated data mining algorithms combining different attributes of measurement data. The peculiarity of this specific study is the focus on the real-time stream management techniques allowing preserving memory about the past happenings and the integral-like developments of the signals. In the interval-based measurement data, the attributes are measured and encrypted by metering observers. For this reason the attributes of information being traced externally by the security agents cannot be manipulated by attackers. Moreover, the Smart Meter Gateway (of NORM meters) will be integrated with the SUCCESS Security Management Solution. The scenario is substantially changed after the adoption of Service Oriented Architectures and Event Driven Architectures (SOA/EDA) such as FI-WARE or similar. In this case, part of the information cannot be encrypted. It is available for both the network agents deputed to optimise the network and to the malicious agents potentially harmful for the network operations. The study will perform the analysis of modalities consuming real-time measurements in order to establish the decision-making and the energy optimization decisions.

In the known state of the art there are currently no solutions available. This study will perform mapping of the available data and the combination of the individual data with the aggregated data made available from other data sources. The expected output is to align security measures taken by different decentralised agents acting from geographically dispersed Multi-Agent System. These data sets coming from smart meters end devices (e.g. NORMs and low cost equivalents of phasors) will be analysed with a focus on reliability, authenticity, real time-ability, and costs. We plan to proof that the data streams from NORMS bears the required significance for the desired evaluation. In the current scenario, this aspect is dominated by the manual operations with smaller data sets. In the new automated Big Data scenario, this functionality should be automated in order to be performed in real time dimension.

When the CSMS will deliver real-time process knowledge about energy measurements, a special focus in phase 2 will be on the detection of malicious Distributed Traffic Patterns. It will result in the capability of the European security monitoring & information system (E-SMIS) to recognise the above-mentioned anomalous patterns. Once it will be done, some attacks on or just misbehaving meters may be recognised only when the traffic or data patterns of many
devices is being analysed. This unit of a work might be transformed in an algorithm implementing novel decentralised control feature. Once this functionality will be ready, it will be used in order to visualise the security status of the observed system at the premises of agents belonging to the MAS.

10.1.6 ENG specific study

The identified countermeasures in WP3, related to devices placed on customer premises or in public places, will be tested to assure security of Smart Meters, e-Car chargers and their communications with DSOs. At this purpose the data containing information about threats and countermeasures will be sent to the data management of E-SMIS. Therefore, we will create a set of services and interfaces that will enable communication from WP3 towards the E-SMIS allowing the correct detection and mitigation of threats at Pan-European monitoring. These services will be linked to the data management Tier 1. The data passed will be exploited from both WP3 and WP4 to match the proper countermeasures once it is established the likelihood of threat/attack occurrences that represent the key indicator to be estimated to compute the risk level of a given threat and the related countermeasure.

10.1.7 P3com specific study

A decisive part of the E-SMIS is the communication system that shall serve both the centralised and the decentralised agents of the E-SMIS. The ability of the E-SMIS to provide real-time insights on the ongoing threats is defined by the efficiency and the structure of the underlying communication network.

The concept takes the specific functional needs of the E-SMIS and its clients (DSOs and TSOs) into consideration, in accordance with the suggested architecture infrastructure in Task 4.2 as well as the communication solutions in Task 4.4. The communication system shall need to be optimised for different loads and types of data.

The concept will be based upon the functional architecture of the E-SMIS. The functional architecture shall consider the needs for both local and centralised data processing and must optimise the communication exchange with respect to load, security and reliability. Optimal network architectures will be inspected and existing infrastructure solutions will be considered in optimizing the interfaces and the information exchange. Requirements on the access layer with a focus on security and performance that will enable real-time data streaming and processing will be considered and if necessary defined.

11. SUCCESS Communication Solution

This chapter documents the result of Task 4.4 of SUCCESS.

The SUCCESS communication solution is based on the evolving LTE infrastructure and 5G networks as solution. The main driving force behind development of 5G is to support wide range of use-cases such as, augmented reality, logistic tracking, energy meters, cell automation, smart factory, transport. In future smart grids and industries use-cases will require ICT infrastructure supporting ultra-low latency, high availability, reliability and longer battery life. These requirements set the scene for next generation of wireless access – 5G systems that are set for commercial availability in 2019. The Figure 11, shows how LTE is evolving and based on the requirements of use cases we are getting closer to the 5G. Key enablers for 5G, including Network slicing, E2E security, NFV, Radio Access, SDN will enable the use of the 5G technology in SUCCESS solution.
11.1 5G Key Enablers

5G systems will be built with key technologies that are understood more on logical instead of physical resources. These technologies enable us to utilise 5G as a communication technology for SUCCESS solution.

11.1.1 5G Radio Access

5G radio enables the wide range of future wireless use cases with customised connectivity. 5G systems will be based on flexible radio-access solution that can support different requirements and deployment types. In 5G radio access, the system will be able to operate in wide frequency spectrum starting from below 1GHz to extremely high frequencies more than 10 GHz. This lower frequency range will enable low latency, ultra-high reliability. While the frequency ranges above 10 GHz will allow delivering extreme data rates and extremely high capacity in dense areas [30].

11.1.2 Network Function Virtualisation

NFV allows a network function to be implemented programmatically instead of by a physical piece of hardware. The most significant benefit brought by NFV is the flexibility to execute network functions independent of their locations. The network functions can be executed in different places for different network slices. By placing network functions accordingly, the same physical hardware can provide connectivity with different latencies [30].

11.1.3 Network Slicing

Current network systems have made it difficult to scale and adapt to changing subscriber demands and meet the requirements of emerging use cases. This has given birth to network slicing which is based on network function virtualisation. Network slicing in 5G enables different users to use communication network facilities with characteristics tailored to their needs. Characteristics such as bandwidth, latency and QoS settings will be customisable. Each slice can have its own management function, security enablers and network topology.

11.1.4 Devices

We distinguish between massive and critical communications scenarios as they have contrasting communications requirements. Depending on the specific use case under consideration, functionality designed for one of these scenarios will be considered as part of a solution.
Massive communication devices need to have very low manufacturing cost, low power consumption and higher scalability. One of the requirements for massive MTC is to provide ultra-long range which is supported by EC-GSM-IoT. It supports 20 dB coverage improvements and can be deployed in the existing GSM networks [28]. NB-IoT technology covers all the components, such as low complexity, low energy and long range. One of the examples for the use of such devices is for connected sensors, AMI.

Critical communication devices require higher availability and reliability along with low latency. Latency reduction technique are standardised in 3GPP release 13 and release 14. Smart grid applications such as grid monitoring and control require very low latency and ultra-reliability which is covered by the LTE evolution. Such devices are suitable for use in intelligent transport systems [29].

The evolution of the devices is shown in Figure 13.

**11.2 Why 5G for SUCCESS?**

SUCCESS is based on designing a new joint Energy and ICT infrastructure with a focus on enabling survivability and resilience by design. To support resilience and survivability by design of system, different components of 5G network architecture will be enabled by the solution. Technology solutions such as Network Function Virtualisation (NFV), SDN and network slicing will enable us to support the vision of the SUCCESS solution. In order to provide both secure and close to real time communication for new energy infrastructure the 5G key enablers explained above need to be examined and enhanced.

5G will enable end to end low latency and high connectivity for a vast range of different applications. At each layer, from devices and gateways to service enablement, enhanced LTE and 5G concepts will be realised as a communication solution. Figure 14 shows the solution architecture for communication. The communication concepts and technologies on the right
side of the diagram are mapped on to the communication conceptual model shown in Figure 6. These concepts will enable us to realise the SUCCESS communication solution.

Figure 14: SUCCESS Communication Solution

Network Function virtualisation allows reconfiguration and isolated working of the network core functionality. This enables real time QoS provisioning of applications. This is important in the context of optimising resource usage and realising the operational efficiency that NFV promises. NFV is an important technology for the 5G core. NFV improves scalability, flexibility, security and rapid deployment.

11.3 Massive and Critical MTC

From the connectivity point of view, device to device communication and device to infrastructure communication solutions including LTE D2D communication technology solution will be realised depending on use case under consideration. Device to device connectivity allows data rate gain, low latency and efficient utilization of the radio resource by cellular offloading. LTE narrowband communications will be considered as part of the solution, depending on the use case in question.

11.4 SUCCESS Communication Solution: Timescale Now, 2020 – 2030

Currently, LTE advanced is in use and 3GPP LTE release 12 has introduced low cost devices, which enable longer battery life with a very low product cost.

In near future until 2020, enhanced LTE capabilities will be introduced. LTE narrow band, 3GPP LTE release 13 and release 14 will introduce more low cost devices and provide better support for them.

The 5G testing phase will start in 2018 and 5G will be commercialised by 2020. 5G will enable the use of network slicing as described earlier in this report. Beyond 2020, 5G capabilities including enhanced radio interfaces, more low cost and low power radio interfaces will be commercially available. Utility specific network slicing will enable utilities to have their own network slice with their own managed services.

In the time period beyond 2030, we anticipate that 5G will be in widespread use and that further enhancements of currently planned 5G functionality will be developed and deployed.
Within the SUCCESS timeline, we can clearly see how the 5G network functionality will enable the vision of SUCCESS.

12. References

13. List of Abbreviations

3GPP 3rd Generation Partnership Project (standardisation body for cellular communication)
4G 4th Generation Mobile Communication Network, a.k.a. LTE
5G 5th Generation Mobile Communication Network
AAA Authentication, Authorisation and Accounting
AES Advanced Encryption Standard
AH Authentication Header
AMI Advanced Metering Infrastructure
API Application Programming Interface
BR-GW Breakout Gateway
CoAP Constrained Application Protocol
dB decibel (measurement unit for signal)
DER Distributed Energy Resources
DG Distribution Grid
dG Distributed Generation
dSE Domain Specific Enabler
dSO Distribution System Operator
DTLS Datagram Transport Layer Security
EC-GSM-IoT Extended Coverage GSM for IoT
EM Energy Management
ENTSO-E European Network of Transmission System Operators for Electricity
E-SMIS European Security Monitoring and Information System
ESP Electronic Security Perimeter
ESP Encapsulating Security Payload
EV Electric Vehicle
GBA Generic Bootstrapping Architecture
GE Generic Enabler
HTTP Hypertext Transfer Protocol
ICT Information and Communication Technology
IED Intelligent Electronic Device
IETF Internet Engineering Task Force
IKE Internet Key Exchange
IoT Internet of Things
IPSec Internet Protocol Security
LV Low Voltage
LTE Long-term Evolution
MV Medium Voltage
NERC North American Electric Reliability Corporation
NAC Network Access Control
NFV Network Functions Virtualisation
NORM New-generation Open Real-time Smart Meter
NB-IOT Narrow-Band Internet-of-Things
PKI Public Key Infrastructure
PV Photo Voltaic
PMU Phase Measurement Unit
PUF Physically Unclonable Function
RBS Radio Base Station
REST Representational State Transfer
RSA Rivest, Shamir und Adleman (asymmetric cryptographical process)
QoS Quality of Service
SCADA Supervisory Control and Data Acquisition
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDN</td>
<td>Software defined Networks</td>
</tr>
<tr>
<td>SHA</td>
<td>Secure Hash Algorithm</td>
</tr>
<tr>
<td>SM</td>
<td>Smart Meter</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>TSO</td>
<td>Transmission System Operator</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>UMP</td>
<td>Utility Management Platform</td>
</tr>
<tr>
<td>WP</td>
<td>Work Package</td>
</tr>
</tbody>
</table>