Communication network interdependencies in smart grids

www.enisa.europa.eu European Union Agency For Network And Information Security

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors and Contributors

Rossella Mattioli, ENISA
Konstantinos Moulinos, ENISA

Contact

For contacting the authors please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

We have received valuable input and feedback from
Maria Pilar TORRES BRUNA, everis Aerospace & Defense - Cybersecurity area
Jose Luis DÍAZ RIVERA, everis Aerospace & Defense - Cybersecurity area
Dr Juan ORTEGA VALIENTE, everis Aerospace & Defense - Cybersecurity area
Alberto DOMINGUEZ SERRA, everis Aerospace & Defense - Cybersecurity area
Carlos Justo ALAMEDA LOPEZ, everis Aerospace & Defense - Cybersecurity area
Ruben SANZ MUÑOZ, S21Sec
Sara GARCÍA-MINA MARTINEZ, everis Aerospace & Defense - Cybersecurity area
Alvaro JIMENEZ, Gamesa
Annabelle LEE, Electric Power Research Institute (EPRI)
Aurelio BLANQUET, EDP Distribuição
Filip GLUSZAK, GridPocket
Geoffrey RIGGS, ENCS
Guillaume TÉTU, Trusted Labs
Hani BANAYOTI, CyberSolace
Jose VALIENTE, CCI
Julien SEBIRE, ENCS
Maksim GLUHHOVTŠENKO, Elektrilevi OÜ
Massimo ROCCA, ENEL
Rajesh NAIR, Swissgrid
Victor BERMÚDEZ, REE
Vytautas BUTRIMAS, Ministry of National Defense, Republic of Lithuania
Finally we thank the experts of ENISA ICS SCADA Stakeholder Group, EuroSCSIE and all participants to the validation workshops held in Madrid the 8th of October 2015 in providing us useful feedback during discussions and interviews.
The study was conducted in cooperation with everis Aerospace & Defense - Cybersecurity area and S21Sec.

978-92-9204-139-7, 978-92-9204-139-7

Contents

Executive Summary

Smart grids can be described as a new generation of smart power networks that integrate actions coming from all connected end-users. This infrastructure provides bidirectional communications between end-users and the grid operator, and therefore extends the attack surface against the power system.

However, one point that has been constantly overlooked and has not received the attention it deserves concerns the interdependencies and communications between all the assets that make up the new power grids. These interdependencies in communications are a fundamental pillar, as they represent the means by which all devices communicate within the smart grid network.

Information transmitted through these intercommunications contains not only customer and consumption data; but also status checks, instructions to execute, orders for devices to redirect power flow, etc. Therefore, their protection is essential to protect the privacy of the customers and prevent attacks which could cause blackouts, power overloads, device malfunctions, data tampering, or even catastrophic cascading effects that could bring down the power grid itself in more than one country.

For this purpose, this study focuses on the evaluation of these interdependencies, and their architectures and connections in order to determine their importance, threats, risks, mitigation factors and possible security measures to implement. To obtain this information, experts in the fields and areas related directly with smart grids were contacted to gather their know-how and expertise.

The concerns that were expressed by these experts can be sorted into two main categories, technical recommendations and organizational recommendations:

- Regarding smart grid devices, these devices are now exposed to different networks, and therefore their periodic update becomes essential in order to ensure that they are protected against the latest threats that appear. Furthermore, these devices should also implement by default security measures to protect them (such as authentication, encryption or frame counters), as implementing such measures in the deployment phase is much more costly and does not reach the same level of security.
- Regarding the communications interdependencies, the main concern is with the protocols used on the smart grids. There is an urgent need to harmonize the current situation by establishing common interconnection protocols to be used by all devices, and ensure that these protocols implement by default enough security measures to protect the data whilst it is in transit (such as encryption or mutual authentication).
- Finally there is the need to align policies, standards and regulations across EU Member States to ensure the overall security of smart grids. This is now even more important due to the risk that cascading failures can cause; as smart grid communication networks are no longer limited by physical or geographical barriers, and an attack on one country could translate into another.

Additionally, due to the global and distributed nature of many of these threats, it becomes necessary for European organizations, distributors, utilities and the rest of involved stakeholders to share knowledge on these attacks both on incident management and incident reporting level.

In conclusion, the protection of the intercommunications in smart grid networks is essential in order to ensure the correct operation of the network and the protection of private and sensitive data. Furthermore, it is necessary in order to protect against attacks to the power grid, therefore making it a matter of national and European interest. For this purpose, the following recommendations have been developed:

Recommendation 1: European Commission should ensure the alignment of policy approaches across EU countries to establish a common posture for smart grid communication interdependencies. Cyber security has become one of the main concerns regarding the implementation of smart grids, and especially concerning the networks used for the interconnection of all the assets that make up this new grid. Therefore, it is inherently necessary to protect these communication networks, the data that is transmitted through them and the devices connected to them. European Commission should ensure the alignment of the requirements and standards for smart grid communication networks, especially regarding the homologation of security devices and protocols.

Recommendation 2: Manufacturers and vendors should foster intercommunication protocol compatibility between devices from different manufacturers and vendors. Currently, many manufacturers and vendors, due to the lack of standards, make use of their own proprietary protocols and communication systems for the intercommunication between their devices. Therefore, when a distributor or utility makes use of these devices, the rest of the network devices have to be provided by the same vendor, or have to be specifically compatible with them. Distributors, utilities and other actors involved should make use of devices acquired from various supply lines without having to be concerned about incompatibilities in the communication among them.

Recommendation 3: European smart grid operators and relevant authorities should develop a set of minimum security requirements to be applied in all communication interdependencies in smart grids. Security controls must be defined to reach a minimum level of security that ensures service connectivity continuity and resilience, both in public and private environments. This could be done by establishing a working group at European level, with representation of all relevant stakeholders, in order to define a series of recommendations regarding the minimum security requirements that should always be applied to smart grid devices, intercommunications and interdependencies.

Recommendation 4: Manufacturers, vendors and asset owners should implement security measures on all devices and protocols that are part, or make use of the smart grid communication network. Traditionally, grid devices and assets were usually isolated, or interconnected through private local networks. However, smart grids bring a new level of interconnection, where devices can be connected to large networks, wireless networks and even the Internet. This leads to the need to protect these communications against eavesdropping and tampering, from the origin and up to the destination. This could be achieved by supporting the implementation of security measures by default on all the protocols used for intercommunication within the smart grid network.

Recommendation 5: Manufacturers, vendors and asset owners should work together on updatable devices and periodic security update support. Nowadays, it is the norm for software and firmware to receive periodic updates to fix vulnerabilities, add new security features or fixes, and even add new capabilities. This is quite common on personal devices and servers, however it is not the case yet in smart grids. Devices must be designed to be easily updated, both their software and firmware, in order to ensure that they maintain an acceptable security level. Manufacturers and vendors should work together on this topic, as they need to design their devices to be easily updatable, and need to develop an update program to maintain them updated.

Recommendation 6: European Commission, Member States and all relevant smart grid stakeholders should promote incident reporting and attack patterns sharing. With the implementation of smart grids, many new attack vectors and network entry points have appeared as a consequence of their intercommunicated and distributed nature. For this reason, it becomes necessary to share data and attack patterns to help all involved agents protect their assets and develop countermeasures which can, in turn, be shared to protect the overall smart grid network.

Recommendation 7: European Commission, Member States and all relevant smart grid stakeholders should promote increased training and awareness campaigns. One of the gripes that threats smart grids is related to the limited number of qualified professionals; a few of the existing ones lacking adequate training regarding security. This is due to in new scenarios that have appeared on energy grids regarding the new features that come with the implementation of smart grid technologies.

Glossary

ADA	Advanced Distribution Automation
AMI	Advanced Metering Infrastructure
AMR	Automated Meter Reading
BAN	Building Area Network
BSS	Business Support Systems
CAPEX	Capital Expenditure
CERT	Computer Emergency Response Team
CIM	Common Information Model
CPN	Customer Premises Networks
CSP	Communication Service Provider
DER	Distributed Energy Resources
DLR	Dynamic Line Rating
DMS	Distribution Management System
DMZ	Demilitarized Zone
DR	Demand Response systems
DSO	Distribution System Operator
EH	Electronic Highway
EMS	Energy Management System
ENTSO-E	European Network of Transmission System Operators for Electricity
ETSI	European Telecommunications Standards Institute
FAN	Field Area Network
FDEMS	Facility Distributed Energy Resources Management System
GIS	Geographic Information System
HAN	Home Area Network
HVDC	High-Voltage Direct Current
IAN	Industrial Area Network
ICCP	Inter Control Centre Protocol
ICT	Information and Communication Technology
IED	Intelligent Electronic Device
ISMS	Information Security Management Systems
ISO	Independent System Operator
MDM	Meter Data Management
NAN	Neighbourhood Area Network
OMS	Outage Management System
OPEX	Operating Expense
OSS	Communication Operations Support Systems
PLC	Power Line Communications / Programmable Logic Controller
PMU	Phasor Measurement Units
REP	Retail Energy Providers
RTO	Regional Transmission Organizations
RTU	Remote Terminal Unit
SCADA	Supervisory Control and Data Acquisition
SLA	Service Level Agreements
TSO	Transmission System Operator
UCTE	Union for the Coordination of the Transmission of Electricity
UCPTE	Union for the Coordination of Production and Transmission of Electricity

WAMS	Wide Area Measurement System
WAN	Wide Area Network

1. Introduction

Smart grids can be described as a new generation smart electric network that integrates actions coming from all connected end-users. This infrastructure provides bidirectional communications between end-users and the grid operator, and therefore extends the attack surface against a power system. For instance, consumers such as households and enterprises are now digitally connected to the ICT infrastructures of Distribution System Operators (DSOs) through smart meters via a Wide Area Network (WAN) network. Smart meters set the demarcation point between the DSO Information and Communication Technology (ICT) infrastructure and the Customer Premises Network.

Smart grids in addition to bringing increased automation and control capabilities to the transmission and distribution grids also add a new layer of system complexity that offer new challenges for insuring the reliability and safety of operations[1]. Existing technologies such as Energy Management System (EMS), Distribution Management System (DMS) and Supervisory Control and Data Acquisition (SCADA) are being updated in order to adapt them to smart grids, alongside the integration of new technologies. Many of these supporting communication infrastructures, particularly WAN communications, are provided by telecommunication operators or Internet Service Providers (ISPs). Therefore these infrastructures will most likely be shared among multiple companies, which bring in multiple interdependency issues, ranging from the reliability of the whole power system to new cyber security risks.

These are just two use cases which prove that communication networks have become essential elements that allow the "smart" aspects of the power grids. They provide real-time knowledge of the grid, perform actions instantaneously when required and gather customer consumption information. These vital assets have to be taken into account especially as far as security is concerned for several reasons: the data they transport, the increasing attack surface, the possible cascading effects that an attack can generate in the rest of the grid, etc.

This report focuses on the aspects related to the communication networks and intercommunications between them in smart grids, identifying vulnerabilities, risks and threat agents. This report makes available a set of recommendations to mitigate identified risks.

1.1 Objectives and Scope

This report presents an analysis of the current situation of smart grid networks, considering the most relevant factors in this case, including: the role networks play in smart grid domains, the main threats affecting these communication infrastructure networks and the interdependencies between networks. Therefore, the following objectives have been set:

1. Review and analyse communication infrastructures in use in smart grids at different domains: end-user premises (HAN, IAN, and BAN), transmission grids, distribution grid, generation (bulk and DER), electric vehicle and other power storage facilities.
2. Study connectivity interdependencies for smart grids among different domains in the electricity system within a Member State (MS) and between MS.
3. Obtain a list of the main threats affecting communication networks in smart grids.

[1] Kun L. and Mathews, R. "Interoperability & Critical Infrastructure Protection: A Review of Activities To Ensure the Reliability of the U.S. Electric Power Grid", *IEEE-USA*, 2007.

4. Evaluate the current situation and possible network attacks with cascading effects on large parts of the population.
5. Collect good security practices and measures for the communication networks (including different channels, technologies and protocols).
6. Analyse, in relation to the identified good security practices, gaps in current implementations of communication networks in all smart grid domains.
7. Explore limiting factors, impairments, constraints and potential incentives for the target audience to deploy these measures.

1.2 Methodology

This study was carried out using a five-step methodology (shown in Figure 1) which begins at the initial information gathering from official sources and experts in the field and ends in the development of a report summarizing the findings and the recommendations to the target audience.

Figure 1: Methodology used to carry out the study.

1. **Identification of experts**: the first step was to identify the experts in the field of smart grid security. In order to obtain varied and well-balanced results, experts from academic, industry and government sectors were selected. Expert representatives from at least half of the EU member states were included in this list.
2. **Desktop Research**: initial research of already published documents in order to get as much information about communication dependencies as possible. Develop a questionnaire which includes the questions needed to achieve the project objectives.
3. **Collecting Experts' and stakeholders' point of view**: During this step, a questionnaire was used internally to guide the interviews with experts. These interviews were carried out during a 6-week period in order to obtain experts' and stakeholders' point of view.
4. **Analysis**: the fourth step was to analyse all the data obtained, including the results of the interviews, gathering initial conclusions.
5. **Conclusions and recommendations**: the last step was to further analyse and contrast these results with the experience of the consortium and external sources.

1.3 Target audience

This report provides information on the networks and interconnections between them in smart grids, aimed at helping operators and manufacturers to understand them, and prepare against possible security risks. Therefore, the target audience is:

- Smart grid operators.
- Smart grid manufacturers and vendors.
- Smart grid security tools providers.

1.4 Structure of this document

This report has been structured as follows:

- **Chapter 1**: brief introduction to the study, lists the objectives and describes the methodology followed on this report.
- **Chapter 2**: Presents the state of the art of communication networks and intercommunications in the different domains of smart grids, detailing the architectures and technologies most commonly used in each one.
- **Chapter 3**: Evaluates the interdependencies that can be found in smart grids and its relation with telecommunication providers and the Internet. This analysis highlights the features of these interdependencies and their relation to the cascade effect threats.
- **Chapter 4**: Presents a specific risk analysis of the specific threats and vulnerabilities that can affect communications in Smart grids, describing them.

2. Key aspects of communication networks in smart grids

This section analyses the communication infrastructures in use in smart grids at different domains: end-user premises, transmission grids, distribution grids and generation.

Figure 2: End-to-End smart grid communications architecture[2].

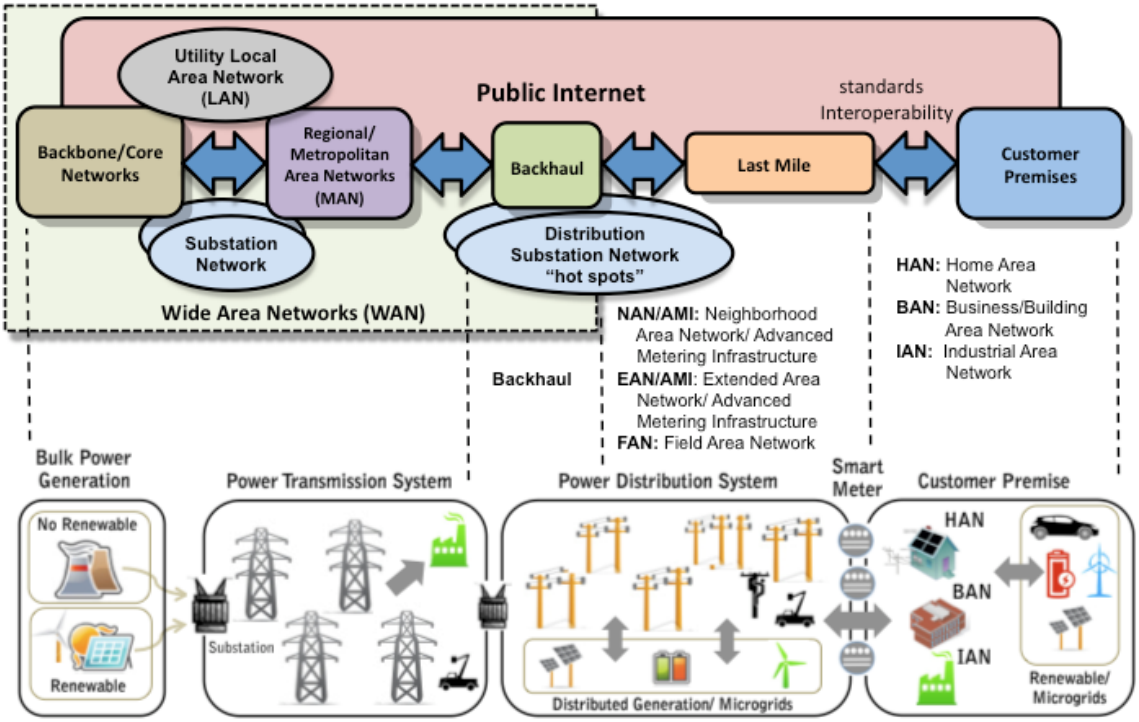


Figure 2 shows an overview of the standard communications architecture of a smart grid. This scenario considers the communications making use of the Internet due to the physical separation between the different sites of each section.

2.1 Customer premises network (CPN)

The customer premises networks[3] are composed of big industries, small and medium business, office buildings, smart buildings (such as modern office buildings) and standard home users. Due to the different natures of these sites, three separate networks have been developed in order to group them: Home Area Networks (HAN), Business/Building Area Networks (BAN) and Industrial Area Networks (IAN).

The **Home Area Network** (HAN) effectively manages the on-demand power requirements of the end-users. This network is envisioned to interconnect smart electric appliances such as televisions, washing machines, or energy management systems. It is the supporting infrastructure for demand-response applications (i.e. switching smart appliances on or off in order to make an efficient use of electric rates) and advanced energy services provided by

[2] IEEE P2030/D.50. "Draft Guide for Smart Grid interoperability of energy technology and information technology and information technology operation with the Electric Power System (EPS), and end-user applications and loads", IEEE SA Standards Board, 2011.
[3] ENISA "Smart Grid Security. Annex I. General concepts and dependencies with ICT", 2012.

DSOs. This network can also provide integration between home automation equipment and energy management systems, and is directly related to the Smart Home concept.

The **Business/Building Area Network** (BAN), or Commercial Area Network, is a communication infrastructure intended to support the needs of regular businesses (e.g. office buildings). The power demand of businesses' buildings is significantly higher than those from households, and its pattern follows a different curve. Business Energy Management Services and Building Automation, as well as other advanced energy services need to be supported by the BAN. On the other hand, a group of HANs is also sometimes called a BAN. In this case, the network includes all communications in one Building due to its size. The BAN network is directly related with the concept of Smart Building.

Finally, the **Industrial Area Network** (IAN) can be defined as the communication infrastructure that allows the interconnection and support of all machines and devices needed in a particular industry, including regular ICT hardware and software (i.e. computers, printers and servers) and Industrial Control Systems (i.e. SCADA, Distributed Control Systems (DCS), Program Logic Controllers (PLC's)).

Architectures and technologies used in CPN

Figure 3 shows the architecture of the network that connects customer premises with data centres on the smart grid. It also shows the different technologies that are most commonly used to interconnect the different devices that make up the network. Note that the PLC mention on Figure 3 refers to "**Power Line Communications**", and does not specify any application protocols.

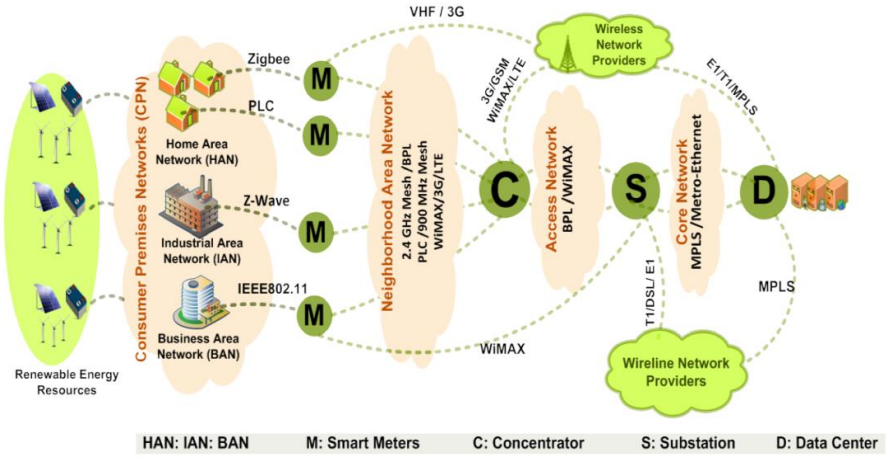


Figure 3: Basic network architecture[4].

Depending on the customer premises' network type (HAN, IAN or BAN), different technologies can be used. For example, one Smart Meter configuration could make use of ZigBee for Home Area Networks, Wi-Fi for Business Area Networks and Z-Wave for Industrial Area Networks; another option is to use the IEC 62056 protocol, based on the DLMS/COSEM protocol, for these communication networks. Therefore, a combination of different technologies can be used in order to manage the needs of the grid interdependencies, based on the specific requirements of the area, infrastructure, etc.

[4] AL-OMAR B. et al. "Role of Information and Communication Technologies in the Smart Grid. Journal of Emerging Trends in Computing and Information Sciences", in *Journal of Emerging Trends in Computing and Information Sciences*, 2012.

2.2 Communication networks in the distribution grid

Historically, distribution systems have included little telemetry, and almost all communications within the domain were performed by humans[3]. It is considered that "the primary sensor base installed in the distribution domain is the customer with a telephone, whose call initiates the dispatch of a field crew to restore power". It was unlikely for distribution substations to be connected to a central SCADA system, and even then these were not automated at all. Electrical substations required manual equipment switching and load, energy consumption and abnormal event data was collected manually. On the other hand, Transmission System Operators (TSOs) have extensive control over transmission-level equipment, which is now being enhanced with a smarter transmission grid.

However, with the arrival of the smart grids, distribution systems are facing a paradigm shift. As it is acknowledged by major industry players "distribution networks are under high pressure to meet requirements for converting their conventional static grids into modern and dynamic smart grids. In particular, the increasing occurrence of decentralized generation (DER) is influencing this trend, as well as the need to improve the quality and reliability in both MV and LV networks" (See Figure 2).

Due to this change, there are new requirements on the automation, monitoring, control and protection of distribution substations and transformer stations/centres. More advanced automation is expected at the distribution grid with the upcoming smart grids. This "extra" automation is basically Advanced Distribution Automation (ADA). The goal of the ADA is the real-time adjustment of the distribution system by changing loads, usually without direct operator intervention, in order to dramatically improve system reliability, quality, and efficiency. In order to achieve this, substation feeder automation and control will play a central role, and will allow DSO's to make the most of DERs, AMIs and Demand-Response strategies, making these three new concepts an essential part of the ADA toolbox.

The **last mile** communication infrastructure of the smart grid is a two-way communication network generally overlaid on top of the power distribution system, which enables features such as: advanced metering services, distribution automation and substation automation. The underlying communication infrastructures are: Neighbourhood Area Network (NAN), Field Area Networks (FAN) and Advanced Metering Infrastructure (AMI), depending on the devices it interconnects and the applications supported. For instance, FANs are used to connect distribution substations, distributed/feeder/transformer centre field devices and DERs/micro-grids, including the utility scale electric storage, to the utility control and operation centre. In addition to these systems, NANs also include smart meters in households, industries and businesses. Likewise, AMIs can be used interchangeably with NANs, but only to interconnect smart meters with back-office systems.

The last mile networks (i.e. AMI, NAN, and FAN) as well as DERs/micro-grids and other distribution substation networks are interconnected with utility control and operations via the **backhaul network**. This network can be owned and managed by the utility (i.e. DSO) or by a third party, such as a public telecommunications service provider. Typically, last mile networks have access to more than one backhaul network. Backhaul networks can use wired or wireless technologies and enable the aggregation and transportation of customer-related smart grid telemetry data, substations automation critical operations data, relevant DER and micro-grid field data, and mobile workforce information.

The **distribution substation network** is an infrastructure that interconnects all devices within a distribution substation. It is comprised of LANs that contain the local SCADA, IEDs, RTUs, PMUs and other field devices that need to be remotely controlled and monitored. At the same time, the distribution substation network provides connectivity to the backhaul network, either directly or through the FAN network, which in turn can interconnect several distribution substations before accessing the backhaul. Transformer centre networks can be seen as a condensed version of a distribution substation network.

The last relevant communication infrastructure supporting power distribution operations and DER/micro-grids is the **feeder network**. This network helps to exchange information with field devices (such as switches, capacitor banks and sensors) and IEDs that are distributed along the power lines, substations and transformer centres. It can be considered as an overlay on the electrical grid and can use both wireless and wired communication technologies.

Architectures and technologies in the distribution grid

Smart grids have brought many changes to traditional power grids, making use of new technologies and devices to enable new features that allow better communication, distribution and overall efficiency[3]. As it has been seen on the previous section, distribution automation provides DSOs with an increased control over distribution-level equipment. However, a more advanced automation is expected at the distribution grid with the upcoming smart grid. Literature refers to this "extra" automation as smart distribution system or Advanced Distribution Automation (ADA).

Apart from this, distribution networks make use of many existing technologies and protocols, depending on the needs of each implementation. ANNEX B summarizes some of the most relevant ones, grouped depending on if they are commonly used on last mile networks or on the backhaul networks. On the other hand, there are others technologies, not directly related to communications, but that have to be considered when evaluating new distribution grids. These are:

- **Fault Detection, Isolation and Restoration** (FDIR) systems are focused on improving the reliability of the distribution networks.
- **Integrated Volt-VAR Control** (IVVC) systems are designed to reduce electric feeder losses improving the overall voltage distribution and conservation in both peak and non-peak time periods.
- **Organic Flash Cycle** (OFC) systems can potentially increase power generation from thermal energy reservoirs

2.3 Communication networks in the transmission grid

Transmission is the bulk transfer of electrical power from generation (and storage) sources to the distribution grid through multiple substations, which are typically operated by TSOs. The main goal of a TSO[3] is to maintain the stability of the electric grid by balancing generation (supply) and load (demand) across the transmission network.

In today's electrical grids, the generation, transmission and sub-transmission segments are performing at a high level and are equipped with automation systems. This has been done by installing Remote Terminal Units (RTUs) and other control devices in substations and generation plants, connected to a Distributed Control System or to centralized SCADA/EMS systems.

Therefore, all these recently implemented automated systems and devices in the substations need to communicate with the central SCADA/EMS systems in order to ensure that they are properly controlled. This requires a new communication infrastructure to enable this communication and allow remote control and regulation of the systems as needed. This is especially important in the case of controlling supply and demand, whether automated or manual, as a failure to control it could potentially cause system overloads or area blackouts.

Additionally, due to the critical nature of these infrastructures, the new communication infrastructures and networks must be secured against unauthorized tampering. This includes not only physical security but, more importantly, cyber-security against the new threats that have appeared as a consequence of the implementation of smart grids (many derived from existing traditional, well known, network threats such as eavesdropping, interception, etc.).

Architectures and technologies used in communication networks in the transmission grid

The automation of the transmission power grid requires the use of specific systems and technologies in order to be controlled. Some of these systems are already in use and are fundamental for the communications of the transmission grid:

- **Distribution Management Systems** (DMS) are a series of applications to monitor and control the entire distribution network entirely, and which are becoming more and more important with the advent of smart grids. These are complemented by SCADA and EMS systems, providing functionalities such as: unbalanced power flow control, distribution state estimation, integrated volt control, fault identification and location, and service restoration. Overall, they provide the means to improve the management operations of the network and allow operators to be able to operate and optimize it in real time.
- **Energy Management Systems** (EMS) are used to analyse and operate the transmission power system reliably and efficiently. Operators using this system can supervise the network topology, connectivity and load conditions (including circuit breakers, switch states and control equipment status).
- **Supervisory Control and Data Acquisition** (SCADA) systems interact with each substation (those that include HMI and RTU devices) and of the entire network. These systems are designed to manage switching, monitoring and control these substations. The SCADA/EMS monitors the status of all circuit breakers (open/closed), to create bus or branch topology configurations of the power system, allowing for optimal power flow calculation, state estimation, contingency analysis, outage scheduling, voltage and stability analysis, alarm processing, etc. Moreover, the SCADA/EMS systems also monitor substation metering technology, to retrieve data on line current and voltage levels at substations.

Apart from these technologies, smart grids will bring a whole range of new specific applications, systems and technologies designed to improve the transmission grid. The most relevant cases are the High-Voltage Direct Current (HVDC), Phasor Measurement Units (PMU), Dynamic Line Rating (DLR) and Wide Area Measurement System (WAMS) technologies, which are described in the following paragraphs:

- **High-Voltage Direct Current** (HVDC) transmission systems use direct current for the bulk transmission of electrical power, in contrast with the common alternating current systems. For long-distance transmissions, HVDC systems can be less expensive and will suffer lower electrical losses.
- **Dynamic Line Rating** (DLR) uses sensors to identify the current carrying capability of a section of the network in real time to optimise utilisation of existing transmission assets, without the risk of causing overloads.
- **Phasor Measurement Units** (PMUs) are devices that provide high quality measurements of bus angles and frequencies using a common time source for synchronisation (i.e. GPS radio clock). PMUs can be autonomous systems or part of a protective relay or other device in a substation. They are capable of detecting faults early, increasing the power quality, enabling load shedding and other load control techniques, etc. PMUs are considered the initial data source for Wide Area Monitoring System (WAMS) applications, essential in regional transmission grids, local distribution grids and even wide super grids.
- **Wide Area Measurement System** (WAMS) make use of advanced measurement technologies in order to monitor and control large power grids and super grids. They can be used as a standalone infrastructure or by complementing other conventional supervision systems, such as SCADA/EMS.

There are several common technologies and protocols that are used for the intercommunication between these devices and the rest of the transmission grid network. One of the most relevant ones is the IEC 61850 protocol family, which is applicable to this grid section. Other relevant protocols used on this grid are also on ANNEX A.

2.4 Communication network integration between generation, transmission and distribution grids

According to the distributed nature of the smart grids, there are different parts of them that need to be interconnected in order to exchange information efficiently. The power grid is operated by many different agents that are connected to the same grid. There are those that generate power, those that transmit power, and those that distribute power to end customers. Some of these operators may carry out more than one of these functions. In order to manage this, the IEC 60870 standard discusses how to exchange information among the smart grid elements[5].

Though there are various proprietary and ad-hoc exchange protocols designed to exchange information among these elements, it is much more common for actors to exchange data with each other using standardized protocols, as it is usually more easy and reliable. Some of these standardized protocols are:

- IEC 60870-6 Inter-Control Centre Communication.
- IEC 61698-13 Common Information Model (CIM) RDF Model exchange format for distribution.
- IEC 61670-452 Common Information Model (CIM) RDF Model exchange format for transmission.

Inter-control centre communications depend on the existing low-level communication infrastructure available between these network elements, such as MPLS, PLC, Satellite, POTS or Leased Lines. The current trend is moving towards the use of IP technologies, either on top of the already existing infrastructure by investing in IP-enabled network, or by contracting virtual networks to ISPs.

For non-real time transmission data, the Common Information Model (CIM) is commonly used, and the IEC 61670-452 standard defines how these data is exported to XML for exchange with other parties. The IEC 61670-5xx series section of the standard defines C and web service profiles for the different data access services, making web services the preferred exchange mechanism for CIM data. Nevertheless, it is not uncommon for XML files to be exchanged using mechanisms other than web services, such as FTP or even plain HTTP POST/PUT requests.

IEC 61968-13 is the distribution equivalent of IEC 61970-452, defined for transmission data, and typically includes information related to assets, work, construction, distribution and outage management. The IEC working group is, however, considering merging or replacing this with IEC 61970-452, as there is a significant overlap between both.

Architectures and technologies used in network interconnections

Communications between the generation, transmission and distribution domains are complex and usually require large communication networks, which make use of many different technologies and protocols to adapt to the individual needs of each section and area. Therefore, there is an inherent need to ensure proper compatibility between them in order to ensure the quality, reliability and security of these intercommunications.

A detailed list of some of the most relevant technologies used for the intercommunication within and between these domains can be found on the table present at ANNEX A of this document as a detailed explanation of each protocol and technology falls outside the scope of this deliverable. As a notable mention, the IEC 61850 protocol family is specially adapted for the integration between grid sections.

[5] Expert Group on the security and resilience of Communication networks and Information systems for Smart Grids. "Work Package 2.3 Research Smart Grid communication protocols and infrastructures to incorporate data security measures", 2012.

3. Telecommunication service providers and interdependencies in smart grids

Many of the communication infrastructures, particularly WAN communications, are provided by telecommunication operators or Internet Service Providers (ISPs). Therefore they might be shared by multiple companies. As it was mentioned on the previous section, one DSO can share the communication infrastructure with a TSO or another DSO, but also with a public company, or a large enterprise belonging to a completely different sector.

The communication infrastructure is deployed in order to share information in the smart grid, where the amount and variety of data is large. Therefore the definition of metadata fields is a complex and cumbersome process. The actors involved in this process can be classified into two categories: those which need the data and those which develop products to deliver the required data. The first group of actors includes, but is not limited to:

- Transmission system operators.
- Distribution system operators.
- Energy retailers.
- Energy services companies.
- Billing organizations.
- Energy regulators.

They are sometimes referred to as driving actors since metadata is created by analysing their input. The second group of actors consists of product manufacturers such as smart meter producers, utility companies, enterprise software developers, B/HAS developers, standard logical model developers, etc. We might refer to them as implementing actors, since they are the ones that make data usable by defining its format according to the definitions given by the driving actors. Metadata management is an important part of the early stages of the system development.

Many actors are involved in metadata management. Examples of data management in the smart grid are: network models which may include electrical transmission or distribution, customer data required to identify customer accounts and service locations, geographic information used to derive network models, assets, work orders, measurements, etc. The *Inter-Domain Analysis of Smart Grid Domain Dependencies Using Domain-Link Matrices*[6] study describes in detail the interdependencies in smart grids.

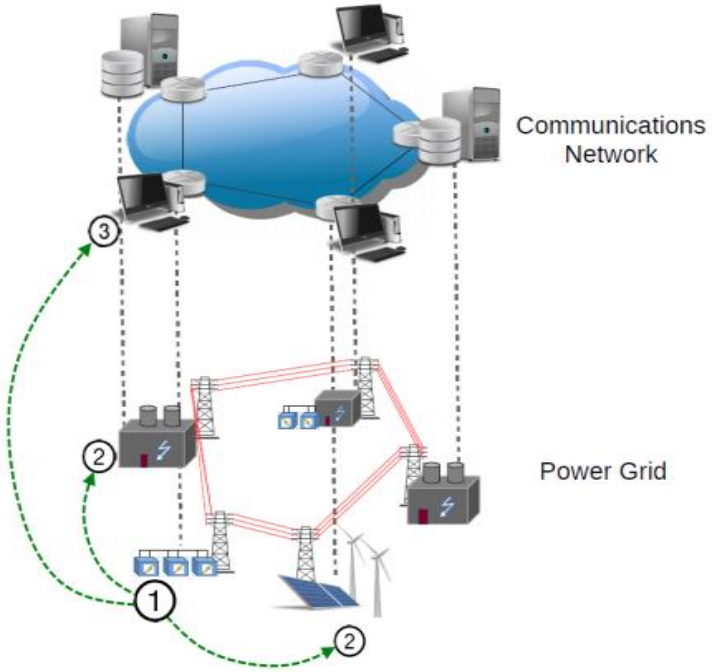
Along the same lines, "*Reducing Cascading Failure Risk by Increasing Infrastructure Network Interdependency*"[7] analyses the importance of improving the security of the interdependencies in smart grids and the need to reduce cascade failures. Although increasingly complex networks have been intensively studied for over a decade, the researchers still focus on the case of an isolated network without external interaction. However, it is known that modern systems are building and working co-ordinately and therefore, these systems must be designed as interdependent networks. A major vulnerability of interdependence networks is that the failure of nodes on a network can lead to failure of child nodes on other networks.

[6] SULEIMAN H. et al. "Inter-Domain Analysis of Smart Grid Domain Dependencies Using Domain-Link Matrices", *Smart Grid, IEEE Transactions*, 2012.
[7] KORKALI M. et al. "Reducing Cascading Failure Risk by Increasing Infrastructure Network Interdependency", *arXiv,* 2015.

When node (substation) or edge (transmission line) failures occur, power re-routes according to Kirchhoff's and Ohm's laws. This re-routing increases flows along parallel paths, which can subsequently trigger long chains of component failures, potentially leading to a wide-area blackout. As a result of this process, failures propagate non-locally: the next component to fail may be hundreds of miles or tens of edges distant from the previous failure leading to a cascade of failures. The research of interdependency issues will lead to the development and application of new system concepts and design approaches towards the mitigation of the risks posed by these interdependencies on a nationwide scale.

Figure 4 represents an example of how a cascade effect might affect the smart grid. Considering a pair of interdependent networks (a power grid and a communication network) in which a fraction of the number of nodes in the power grid are coupled to corresponding nodes in communication network. When a node fails in this model, the associated edges in both networks immediately fail too.

Figure 4: A disturbance in (1) causes edge failures (2) in the power grid, as well as node and edge failures (3) in the communication network.



As mentioned in reports "*Catastrophic cascade of failures in interdependent networks*"[8] and "*R&D Themes for Cyber Security in the Smart Grid*"[9], it is very important for inter-operators to consider and become aware of the risks posed by the existence of interdependencies in smart grid communication networks. This is needed in order to prevent the possibility of cascading failures leading towards catastrophic blackouts.

3.1 Inter-operator and multiple communication service providers for smart grid segment networks

Continuing on towards intercommunications and the multiple providers in charge of the specific communication networks from each domain, it is necessary to consider that each one may make use of different technologies and

[8] BULDYREV S.V. et al. "Catastrophic cascade of failures in interdependent networks", *Nature*, 2010.
[9] GHANSAH I. et al. "R & D Themes for Cyber Security in the Smart Grid", 2010.

operation methods. This leads to unique interdependencies among these networks that require cyber-security elements that can impact on the reliability of the rest of the elements of the power system. The correct security design for each one of the services and domains must be one of the main objectives when securing these interconnections[10].

As previously discussed in the section **2.3**, in order to perform the metering and transmission services, operators must use communication networks, Neighbourhood Area Network (NAN), Field Area Networks (FAN) and Advanced Metering Infrastructure (AMI) are interconnected by backhaul networks. The backhaul might be owned and managed by operators and can use wire line or wireless technologies like Wi-Fi, WiMAX, 3G mobile networks and LTE/4G.

The document titled *Advanced Wireless Backhaul for the Smart Grid*[11] suggests that last mile communication infrastructures can be implemented as a backhaul network as long as the following stages are fully implemented:

- Connect all individual meters to local collection points.
- The local collection points have to be backhauled in order to reach a higher capacity level on the aggregation points.
- Aggregation points have to be backhauled to the utility's network operations' centre.

Furthermore, the inter-operator communication network has to connect with several of the following domains, depending on the needs of each individual implementation:

- Last **mile communications network**, which includes all of the individual meters, collection points and aggregation points.
- The **distribution substation network**, where devices connect with distribution substations that, at the same time, are connected to the core backhauled network.
- **Distributed Energy Resources**: their network has many other operators that have to be interconnected with each other and with utilities. Figure 4 on ANNEX D shows that the highest level of the DER architecture (level 5) contains Transmission and Market Operations, and involves a larger utility environment. Regional Transmission Organizations (RTOs) and Independent System Operators (ISOs) need to exchange information about the capabilities and operational status of larger, or aggregated, DER systems. The energy transmissions from the DERs are at the same time interconnected to the demand and response systems, as well as to the utilities' network operation centres.

The network operation centres of the utility companies are the main points from where all the information of the backhauled network in the smart grid begins and flows. These are also the main points where the system operators (control and data centre) are connected. The service of the operators at this point is to act as resource options for balancing supply and demand. This demand and response communication needs to be implemented with a high range of security and tidy protocols. The previous document mentioned[12] underlines how the IEC-61968 standard is considered as an example focused on integration of applications related to transmission, generation, and energy markets. Also, "*Object linking and embedding for Process Control*" (OPC) is an integration standard used for process control integration. It's a requirement that in the inter-operator communication networks, different operators must

[10] ANGELETTI V. et al. "Italian Case Study: socio-economic impact analysis of a cyber-attack to a power plant in an Italian scenario. Cost and benefit estimation of CIPS standard adoptions", 2014.
[11] Solution Brief, "Advanced Wireless Backhaul for the Smart Grid", *CERAGON,* 2014.
[12] ENISA. "Communication networks dependencies in Smart Grids", 2014.

be organized between each other not only in communication network protocols and standards but also in security incidents.

In the bulk generation, transmission, and distribution domains, various control messages and received messages from the distributed sensors in the smart grid are frequently conveyed from the control applications in the control centre to various locations on the smart meter by using a robust communication infrastructure. Demand and response messages in the smart grid are used to provide an interface to connect a variety of users, devices and systems together. There are many messages exchanged through the communication system of the smart grid, such as energy readings from smart meters, triggering events, control messages, device status messages, energy consumption messages, pricing messages, outage messages, etc. Interfaces are used to exchange energy-related information and provide connection among home networks and external networks and systems, such as the utility network. The Internet gateway is considered as an example of such a system, which enables customers' interactions by sending and receiving requests via secure web-portals, this will be described in "*3.3 The role of the Internet in smart grids*".

Within the transmission and distribution domains, the IEC Common Information Model (CIM) has been adopted to allow application software to exchange information about the configuration and the status of an electrical network. The CIM aims to govern several areas pertaining to the physical infrastructure of the smart meters. Some of the areas covered include asset measurements, which are received from telemetry and help to identify the current state of both the assets and the infrastructure. The modern communications infrastructure is used to achieve this task using two-way communication interfaces (backhaul network). One noteworthy example is the data collection from Remote Terminal Units within the SCADA network, which is then transferred to the control centre (system operator). The SCADA database is monitored and updated remotely; therefore database-centric applications are fundamental. One of the IEC standards, IEC 61970-301, defined the core packages of the CIM with focus on the electricity transmission needs, such as EMS, SCADA, and other related applications. In addition, IEC 60870-6 is commonly used to provide data links to exchange measured values among the control centres. It is commonly known as TASE.2 and the Inter Control Centre Protocol (ICCP).

Smart grids can be quite large and geographically dispersed[13]; more importantly, regardless of the distance they still require real-time information in order to automatically manage the different sections of the grid and maintain good efficiency levels. This however requires that power companies convert their existing legacy grids into the new smart grids, requiring in many cases large investments and redesigns of entire sections. A trend has already appeared regarding companies acquiring communication services from third-party communication service providers in order to reduce these costs.

As far as security is concerned, there are some points to consider regarding power utilities and Communication Service Providers (CSPs). By using CSPs to meet the connectivity needs of smart grids, these become dependent on them in order to carry out their work functions. For this reason, it is heavily recommended to not depend on a single CSP, instead make use of several ones, and consider the following points:

- Regarding **Risk Management**, the risk generated by using a single CSP is considerably lower in case of CSP failure or attack, when the dependency of the CSP is minimized, allowing that some parts of the smart grids can avoid being affected.
- **Geographical effectiveness**: The smart grid components can follow different strategies in different places. The usage of different CSPs provides the flexibility of selecting the most expert CSP according to the required technologies and features of the place.

[13] CEN-CENELEC-ETSI, "SGAM User Manual - Applying, testing & refining the Smart Grid Architecture Model", *Smart Grid Coordination Group*, 2014.

- **Technologic Variety**: Using different CSPs allows using different technologies for different network segments within the same domain. This reduces the exposure in case of "Zero-day vulnerabilities" and the cost of dealing with them if they ever occur. Regarding wireless communications, sometimes the usage of different CSPs allows the use of different working frequencies that enhance the wireless communications' security.
- **Isolating** different types of **traffic** and applying different **Quality of Service (QoS)** levels can be done according to data needs, and this practise also provides a mechanism of protecting the information regarding internal power utility processes, or as a "backup" service provider.

However, using different CSPs also has some disadvantages that have to be considered:

- This practice can be more difficult to manage for the power utility, such as the security management (encryption, redundancy, etc.) of the customer data as well as the locations where it is stored (several third-party information systems).
- The operation cost of using multiple CSPs is significantly higher than using just one and it can happen that the network infrastructure for managing different CSPs is more complex and expensive than if only one CSP was used.
- The number of people that have access to confidential information of the power utility is much higher in a scenario with more than one CSP. Consequently, the attack surface for information leakage is much bigger.

Finally taking into account the different points of view that have been discussed in this section, the conclusion moves towards recommending the use of multiple CSPs to provide communications in smart grids, as well as considering possible measures to mitigate the effects of the disadvantages they imply.

3.2 Inter-Member State power infrastructures supporting communication networks

Another important factor that has to be taken into account is the Inter-Member State power infrastructures that support the communication networks, as they now become an essential part of smart grids due to their delocalized nature. Smart grids are no longer confined to a single country; now they have become part of a whole grid spanning throughout Europe, having intercommunication among the different States and reaching a point where a failure or attack in one of them could adversely affect the rest.

For this purpose, the European Network of Transmission System Operators for Electricity (ENTSO-E)[14] has become involved in this process, supporting not only traditional energy distribution, but also focusing on the intercommunications among their systems (see Figure 5).

[14] BARTOSZEWICZ-BURCZY H. et al. "Polish case study. Scenario based assessment of costs and benefits of adoption of comprehensive CIP standards", 2014.

Figure 5: Map of ENTSO-E systems.

ENTSO-E established that the operation of interconnected networks is founded on the principle that each partner is responsible of its own network (coordination at regional and European levels, interference of national system and corresponding inter-TSO coordination that requests more and more coordination), but cannot ignore the rest of the networks. For this purpose, ENTSO-E has developed an Operation Handbook[15] that defines the basic interconnection principles and infrastructure that should be followed in order to establish successful and secure interconnections between grids. It defines the use of the Electronic Highway (EH), a routed network separate from the Internet that interconnects TSOs, can be used for real-time and non-real-time communications. This operational handbook defines a series of points that Transmission System Operators should follow:

- A set of minimum requirements to apply.
- Up-to-date implementation rules and recommendations.
- Common specifications for communications and data exchange.
- Operation and maintenance recommendations.

However, the Operation Handbook does not specify the national grid codes, as this remains responsibility of each country and is usually influenced by market rules. Regarding security, there are a series of recommendations that have been included in order to protect the systems against attacks, and especially against the risk of cascading effects on parts of the network or even the whole network itself. These recommendations are:

- **Connection to the Internet**: there should not be any physical or logical connection between the Electronic Highway (EH) and the Internet. If needed, data exchange between the EH and the outside world should only be done through clearly defined and fully protected limited channels. This can be achieved by using intermediate gateways and firewalls crossing TSO boundaries. Operators however should be aware of recent research on

[15] ENTSO-E. "Operation Handbook. P6 - Policy 6: Communication Infrastructure", 2008.

the visibility of control systems assumed to be disconnected from the Internet. Project Shine [16 and17] for example gave reason to question such assumptions. Operators of increasingly complex systems need to test and check for the possible visibility of devices.

- **Private Networks**: the Electronic Highway can be considered as a private network, as it is isolated from the rest of the networks and the Internet. Only protocols specified by the TRM (Electronic Highway Technical Reference Manual) should be used. Point-to-point connections should be used to interconnect devices through the EH network.
- **Dedicated network for data exchange**: The EH is the main and preferred communication channel for data exchanges among TSOs related to operation. The EH should also be used as communication media for data exchanges among TSOs related to market.
- **Incorporation of new protocols and applications**: it is possible to add new protocols, apart from the ones predefined on the TRM; however it has to be done following the process defined on it.
- **Requirement for EH interconnections**: several standard requirements have been defined, being the following the most relevant ones:
    - Communication redundancy should always be ensured, by using more than one point-to-point lines for each TSO. This guarantees the stability of the EH backbone.
    - Speed and availability should also be controlled in order to obtain stable communications.
    - All data exchanged must be transmitted over the EH from the sender to the recipient uncorrupted, in sequence and in a timely manner to guarantee integrity.
- **TSOs responsibilities**: the following responsibilities have been established for TSOs for the security operation of the EH network:
    - Take appropriate measures to protect the Electronic Highway and each connected TSO against any potential risks such as operation disruption or data corruption and disclosure of confidential data.
    - Protect against any unauthorised access to the EH.
    - Perform periodic malware checks.
    - Monitor and guarantee the availability of EH components in their domain.
    - Check physical line and SCADA connection redundancy.
    - Manage their own network components (such as routers, gateways or physical lines).

Finally, it is important to remember that smart grid assets, even if they are not connected to the Internet, are still vulnerable. The false belief that devices not connected to the Internet are not vulnerable has been an IT myth for quite some time, and one that should be quickly dismissed as reality has proved it otherwise. In a recent report made by the German Government Federal IT Department[18], a cyber-intrusion on a steel mill systems caused physical damage to some of the assets, even though these systems had been isolated from the Internet as much as possible.

[16] Project SHINE (*SHodan INtelligence Extraction*), "Findings report", 2014. Retrieved on the 21-09-2015 from: http://www.slideshare.net/BobRadvanovsky/project-shine-findings-report-dated-1oct2014

[17] Radvanovsky, B. and Brodsky, J. "Project SHINE: What we discovered and why you should care", *ICS Security Summit*, 2015. Retrieved on the 21-09-2015 from: https://files.sans.org/summit/ics2015/PDFs/Project_SHINE_What_We_Discovered_and_Why_You_Should_Care_Bob_Radvanovsky_Infracritical.pdf

[18] Section 3.3.1, "APT attack on industrial installations in Germany", The State of IT Security in Germany 2014. Retrieved 21-09-2015 from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitys ituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile

3.3 The role of the Internet in smart grids

Traditionally, power companies had their own systems designed to control and manage their operations; while many of these systems had been isolated or connected to local private communication networks. Therefore, these companies were in charge and control of all aspects of their systems and, from a security point of view, their main concern was the physical protection of their assets and installations. Therefore, communications were limited and were not exposed to external shared networks, much less to the Internet.

The appearance and exponential growth of the Internet gave way to new means of communications, not only traditional point-to-point ones, which offered a lot of benefits at an affordable cost. Smart grids make use of intercommunication networks in order to interconnect all the devices that make it up, and therefore the need to use large communication networks becomes a basic requisite.

Therefore, the Internet has become one of the main means for smart grids to interconnect their devices, as it provides wide coverage and compatible protocols supported by many different services, enabling direct communication to devices located geographically apart without the expenses of implementing their own communication network (which can be prohibitively high in case of large distributed or nation-wide grids). Furthermore, the use of these communication channels enables smart grids to automatically control and manage all the devices that are part of it, obtaining improved efficiency for the power generation, transmission and distribution, and the overall working of the grid itself. An exception to this point is the Electronic highway, which is focused specially on the use of a private network separated from the Internet for the communications and data exchange between Transmission System Operators, as it has been defined on Section 3.2.

However, these networks, and especially the Internet which encompasses all of them (except the Electronic Highway presented in the previous chapter), are not inherently safe against threats and vulnerabilities. On the contrary, these networks may suffer from a multitude of attacks and are vulnerable to many varied threats to the communications that pass through them (as described in more detail on Section 4.1); this includes not only intentional attacks, but also unintentional data damage caused by employees or badly configured devices.

There are also resilience and security concerns regarding the infrastructure of the Internet itself, as they pose a risk as serious as those that affect the communications that pass through them. These threats were defined by *ENISA's Internet Infrastructure Security and Resilience Reference Group*[19], where they were sorted into three main categories: routing attacks, DNS attacks and Denial of Service attacks (these will also be described in more detail in Section 4.1).

Therefore their securitization becomes a must. As many of these threats and risks are common to the various services that make use of the network, smart grid manufacturers, vendors, operators and experts can take this know-how and existing knowledge in order to adapt and protect and properly configure their own devices against these threats.

In light of these concerns, the risks to power grids have to be thoroughly considered, as they are critical infrastructures that maintain many other systems and services, and are a fundamental requirement for the operation of business, industries and even for the well-being of the population. An even bigger risk appears due to the interconnected and distributed nature of these systems, the cascade effect: a failure or service outage on one distributor or one country, if not properly controlled, could affect other distributors and countries.

[19] ENISA https://resilience.enisa.europa.eu/internet-infrastructure-security-and-resilience-reference-group/threats

Architectures and technologies used for intercommunications through the Internet

The Internet has become the network of networks, a massive grid that connects the whole world together; communications from one side of the world to the other takes less than a second. To maintain such large infrastructures, different architectures and technologies are used; but always following a compatible structure to ensure the compatibility of all the systems and devices that are connected to it.

The Internet makes use of many different architectures and technologies for the different sections that make it up, as well as having available a wide range of protocols that can be used to offer different services and functionalities. The architecture of the Internet is distributed and redundant, there are no established hard point-to-point lines; connections are established using the most efficient path, and so connections to the same destination can make use of different intermediate devices and communication lines each time.

When the Internet was initially envisioned, security was not a concern as the scope was limited; therefore the resulting architecture and protocols proved highly efficient and scalable, but offered no security measures at all by default. Further iterations of these architectures and protocols began to implement security measures for the protection of all the communications, transmissions and services offered through the Internet (such as SSL/TLS, mutual authentication, point-to-point encryption or certificates).

Among all technologies that are available on the Internet, the most relevant ones that are used for communications among the devices part of the smart grid are:

- **Internet Protocol** (IP): is probably the most used and important communication network protocol used by the devices part of the smart grid. This protocol is used due to its compatibility and open-source implementation, allowing different devices from different manufacturers to communicate with ease. Through the use of this protocol, devices can reliably exchange data and manage operations and activities. This protocol however, is vulnerable to a wide range of attacks due to its lack of security measures, and therefore it becomes necessary to implement additional security measures, such as using TLS to encrypt the data, in order to ensure the integrity and confidentiality of the transmitted information or instructions.
- **Multi-Protocol Label Switching** (MPLS): is used to encapsulate various network protocols, and transmit those using short paths to reach the destination, instead of using a long path the whole way. This protocol is scalable, and works independently of the protocol that is transmitted.

There are a series of relevant protocols that can also be used on these networks, in conjunction with the previously listed technologies:

- **Distributed Network Protocol** (DNP): is a set of communication protocols designed specifically for the communication of devices part of automated systems. It is used mainly in SCADA systems to interconnect the Master Station with the RTUs and IEDS. It has been designed to be reliable, but lacks security measures.
- **IEC 61850**: is a standard designed to be used to control the automation processes on electrical substations. It defines data exchange between control systems the substations themselves. It includes many required features to carry out these functions, including data modelling, data storage (substation configuration language, or SCL), fast transfer events and reporting schemes. It also includes variations of this protocol for different installations, such as Hydroelectric Power Plants (IEC 61850-7-410) or Distribution Automation Systems (IEC 61850-7-420).
- **IEC 60870**: defines the systems needed for the supervision and data acquisition of power automation systems. It has been divided into five parts: transmission frame formats, datalink transmission services, general application data structure, coding definitions for information elements and basic application functionalities.

Therefore, not all the technologies and protocols used for the communications through the Internet support security measures by default, and as such it becomes necessary to use additional measures in order to protect them. Some of the most common security technologies that can be used to protect communications include:

- **Transport Layer Security** (TLS): is a cryptographic protocol designed to protect communications over a network. This is achieved by using asymmetric cryptography and client certificates to authenticate both the sender and the recipient and symmetric protocols to carry out data encryption. Its predecessor, SSL v3 is also commonly used, although its use is not recommended due to several security flaws that have been detected on it.
- **IEC 62351**: is a standard designed to handle the security of several protocols including IEC 60870, IETC 61850, IEC 61970 and IEC 61968. Among its features, it includes TLS encryption, node authentication, message authentication and several other specific security profiles.
- **IEV IEC 61850-90-12**: provides definitions, guidelines and recommendations for the engineering of WANs, especially regarding their protection, control and monitoring. It is based on IEC 61850 and several related protocol standards. It is mostly used for communications between substations and the control centre.
- **Internet Protocol Security** (IPSec): comprises of a set of protocols designed specifically to protect IP communications by applying authentication and encryption to them. It supports mutual authentication, and works on the Internet Layer (while TLS works on a higher level, on the Application Layer).
- **Secure Shell** (SSH): is a protocol that provides a secure connection to remote machines, by applying encryption to protect the data. For this communication, the remote machine must have an operational SSH server to which the client will connect to.
- **DNP3 Secure**: is an upgrade to the standard DNP3 protocol designed to provide additional security measures, including authentication and data encryption. It is compliant with IEC 62351-5 standard, and in some cases Virtual Private Networks (VPNs) are also used to secure IP networks.
- **Virtual Private Network** (VPN): is not a protocol per-se, it is more of a concept, but it can be considered as a relevant security measure in order to protect communications. In a VPN the use of point-to-point private network over a public network or the Internet are specified. A VPN uses tunnelling protocols to make available private communication, and to also make use of encryption protocols to protect the confidentiality of the data transmitted.

4. Threat and risk analysis on communication networks in smart grids

This chapter focuses on security threats, risk factors, incidents and attacks affecting communication networks in smart grids, with particular interest on those that might imply cascading effects on large part of the population. Regarding risk factors, some examples include: interconnected networks and systems, communication protocol vulnerabilities or IT vulnerabilities, legacy communication protocols, communication disruptions, malicious software and firmware, compromised hardware, increased number of entry points and paths, new sensitive personal data.

4.1 Analysis and summary of threats affecting smart grid communications

Starting from "*Smart Grid Security: Threats, Vulnerabilities and Solutions*"[20] and "*Smart Grid Threat Landscape and Good Practice Guide*"[21], the goal of this section is to combine the most important aspects of these documents, the experts' interviews and other relevant documents, in order to reach a complete overview of threats that affect smart grids nowadays.

Smart grids bring improvements and better capabilities to the traditional power network. **These networks provide electricity on demand using information and communication technologies that enable energy providers to control the power supply and allow for an efficient power delivery with lower costs**. However, this makes networks more complex and vulnerable to different types of attacks and even unintentional failures due to increased complexity of systems and levels of cyber fragility. The principal difference between traditional grids and Smart grids is that there are three new main security objectives that must be taken in account: availability of the service, integrity of transmitted data and confidentiality of the consumer's data.

However, due to the recent Smart grid concept and implementation there is very little practical experience on cyber-attacks affecting Smart grids. Besides, industrial cyber security is also a quite new topic and security experts are still learning it, developing hacking tools and finding new vulnerabilities at an exponential rate. These vulnerabilities might allow attackers to obtain back-doors, compromise the confidentiality and integrity of the information, and even make the service unavailable. Therefore, the security of traditional and new Smart grid ICT technologies must be addressed by the energy sector. This is not only a task for grid operators but also for public bodies, standardisation organisations, service providers, and any other stakeholder involved. In addition, cyber security must be considered in all Smart grid domains and at all phases of the system life cycle.

As a result of the experience of a cyber-attack affecting a Smart grid, in the "*Smart Grid Security - Annex II*"[22] by ENISA it is underlined how physical security and safety is much more stable and well-known by the actors involved in the Smart grid deployment. For instance, there is abundant statistical data about natural disasters, such as hurricanes or earthquakes, which makes it much easier for experts to characterise these threats from a risk point of view. Alternatively, natural disasters are random events while cyber threats depend on people (i.e. attackers): their motivations, capabilities, interests, etc. Besides, all these factors change over time. As a result, managing risks deriving from cyber security threats is a real challenge that needs to be addressed and solved. In order to succeed in such task it is important to first identify potential threats, at all levels, ranging from natural disasters to technical aspects. When identifying threats, it should not only be considered those targeting infrastructure operations, but

[20] ALOULA F. et al. "Smart Grid Security: Threats, Vulnerabilities and Solutions", International Journal of Smart Grid and Clean Energy, 2012.
[21] ENISA "Smart Grid Threat Landscape and Good Practice Guide", *ENISA*, 2013.
[22] ENISA "Smart Grid Security. Annex II. Security aspects of the smart grid", 2012.

also those targeting the end consumer (i.e. privacy aspects) as well as national security related factors (i.e. government personnel, other national facilities, assets, and interests identified by national intelligence, etc.).

On a similar point, it is also relevant to consider the threat posed by unintentional events that could impact on the security of the systems, assets and intercommunications. While these events cannot be considered as the main topic of the study, rather more alongside it, they still have to be considered when developing general security recommendations. The paper "*Interoperability & Critical Infrastructure Protection: A Review of Activities to Ensure the Reliability of the U.S. Power Grid*"[1] makes a case of the risks posed by unintentional events and incidents and the threat they present to smart grids.

Therefore, based on the threat domains defined on "*Smart Grid Threat Landscape and Good Practice Guide*"[21], the following table (Figure 6) has been developed and expanded in order to cover all the threats that directly affect Smart grid intercommunication networks. The details of each one of these attacks can be found on ANNEX B.

Figure 6: Main threats to Smart grid intercommunications.

CATEGORY	THREAT	VARIANTS	ASSETS AFFECTED
Nefarious activity	Advanced Persistent Threats (APTs)	N/A	Overall systems
	Channel jamming	Distributed denial of service	Communication networks
	DNS attacks	DNS spoofing / poisoning DNS registrar hijacking	Communication networks
	Generation and use of rogue certificates	N/A	End-user systems
	Identity theft	N/A	Personnel and operators
	Injection attacks	Malicious code injection Malformed data injection	End-point systems
	Malicious code	Exploit kits Virus/Worms/Trojans/Malware	End-point systems
	Social engineering	Phishing	Internal/sensitive information Personnel and operators
	Unauthorized access to systems	Privilege escalation Password attacks Unauthorized software installation Use of restricted software	End-point systems Internal/sensitive information
	Web-based attacks	Administration interfaces Web services/applications	Control systems End-point system applications
Eavesdropping, interception and hijacking	Information theft	N/A	Internal/sensitive information
	Man-in-the-Middle (MITM)	Session hijacking MITM Masquerade Mobile network interception Wireless network interception	Internal/sensitive information Communication networks
	Network reconnaissance	Information gathering	Internal/sensitive information
	Replay of messages	N/A	Communication networks

			End-point system interfaces
	Routing attacks	Autonomous System (AS) hijacking Address space hijacking Route leaks	Communication networks
	Smart Meter connection hijacking	N/A	End-point systems
	War driving	War flying	Communication networks Internal/sensitive information
Deliberate data damage	Information integrity loss	N/A	Internal/sensitive information
	Information leakage	N/A	Internal/sensitive information
	Information manipulation	N/A	Internal/sensitive information
	Trusted firmware	N/A	End-point systems Communication networks
Unintentional data damage	Channel interference	N/A	Communication networks
	Configuration errors	N/A	End-point systems Control systems
	Erroneous information sharing	Unintentional information leakage	Internal/sensitive information
	Erroneous use of devices	Systems Administration interfaces	End-point systems Control systems
	Unintentional data alteration	N/A	Internal/sensitive information
	Usage of information from unreliable sources	N/A	End-point systems
Outages	Communication system (network) outage	Network outage cascade effect	Communication networks
	Energy supply outage	Energy supply outage cascade effect	Communication networks
Other threats	Deliberate physical attacks	N/A	End-point systems Communication systems
	Failures & malfunctions	N/A	All systems Communication networks
	Natural disasters	N/A	All systems Communication networks
	Future disruptive technologies	Quantum Computing	End-point systems Communication networks Internal/sensitive information
	Unintentional events	Unintentional data corruption Unintentional data leakage Unintentional misconfigurations	All systems Communication networks

4.2 Common vulnerabilities and risk factors in smart grid communication networks

Following on from the previous section regarding the analysis of current threats, the next logical step is to evaluate the vulnerabilities that affect these systems, based on the knowledge provided by the experts consulted.

It is important to emphasise the fact that most security vulnerabilities in communication infrastructures require defining specific security measures to mitigate them such as: automating system data protection, identifying and enhancing a security perimeter, building comprehensive security through defence-in-depth, and restricting access to data and services to authenticated users based on operational requirements.

Many of these vulnerabilities result from deficient or non-existent security configuration options in the organizations' Smart grid, employees' mistakes, and workers attrition in system automation. Also, the industry is not quite aware about the threat environment and attacker capabilities, underestimating the risk that they are going to have to deal with. Following on from the previous chapter regarding the analysis of current threats, the next step is to list known vulnerabilities that could pose a serious risk to Smart grids, according to the ideas presented on the document by Aloula[20]:

- **Vulnerable consumers*:*** The intelligent devices of the Smart grids can process massive amounts of data and send it to the utility company, consumer, and service providers. As a result, preserving authorized restrictions on information access and disclosure is fundamental in order to protect proprietary and personal data privacy. This is particularly necessary to prevent unauthorized disclosure of information that is not open to the public and individuals and to implement robust transmission methods and protocols. This is extremely important, due to the fact that transmitted information includes private consumer data, which could potentially reveal consumer's activities, devices being used, or consumption habits.
- **Massive number of devices**: Smart grid networks have several intelligent devices that are involved in managing both electricity supply and network demand. This is due to the great area covered on the grids' deployment, with many features and services that must be covered. Moreover, the sheer size of the network makes monitoring and managing it extremely difficult to carry out. On the other hand, a modification or update on these devices can lead to a great economic cost and many staff working hours due to the need to travel to the remote device location. These vulnerabilities could result in intelligent devices being used as attack entry points into the network. If attackers gain access to these machines, they can potentially steal confidential and private data through them, or even manipulate the transmitted information.
- **Coexistence of legacy and new devices**: It is quite usual that legacy devices are in service along with more contemporary ones. This coexistence between devices may result in possible incompatibilities at physical and protocol levels; or even vulnerabilities and threats as a result of possible interdependencies between devices and networks. These legacy devices could become weak points and even cause severe conflicts with current power systems, unless specific security measures are implemented on them in order to mitigate these risks.
- **Implicit trust M2M by default**: Several devices in their Machine to Machine (M2M) communications use implicit trust by default. This is an important weakness due to the interdependency with the other machine lead to the appearance of additional vulnerabilities. If an attacker gains control of the other machine involved, or pretends to be it, he could send wrong data to the first machine or receive confidential and private data from it. Data Spoofing is a threat for Device-to-Device communication in control systems; the state of one device involves the actions of another. Even more, this implicit trust can be used by attackers to carry out Man-in-the-Middle attacks, compromising the network interconnection between these devices and even the rest of the network.
- **Commercial hardware and software**: Commercial hardware and software development is usually done separately from the operators who will make use of it later. This lack of interaction becomes an issue later when these operators proceed to implement security measures to protect the devices and the communications between them, sometimes being unable to fully implement them Therefore, using commercial assets entails vulnerabilities inherent to the hardware and software such as bugs, weaknesses, back-doors, failures or even outdated assets, which present a serious vulnerability for smart grid communications.

- **Communication protocols**: Communications between devices in the Smart grids, especially in the consumer domain, are done through well-known communication protocols. Besides, these protocols have been a long time in use and they are widespread. For example, some of the wireless protocols used in Smart grids (i.e. Bluetooth, ZigBee, Infrared, WiMAX, Wi-Fi, LTE, UMTS or GPRS) are already widely used in other contexts. Therefore, protocols applied on Smart grids are also an important source of vulnerabilities, and many of these vulnerabilities are well known by attackers, and they have even developed automated tools for easing these attacks. Also, many application-level protocols have been designed without adequate levels of intrinsic security mechanisms.
- **Human factors**: All organisations have information that would put business operations at risk in the event that it was to be lost or corrupted in some way. Power grid companies are not exempt; most of their workers are dependent on their computer systems for the success of their businesses and know that cyber threats are increasing, nationally and internationally. Protecting these systems is costly. Even with the increasing sophistication of cyber-attacks from outside sources, the greatest proportion of data losses and failures are still caused by human errors. Many of these can easily be avoided once people become knowledgeable of the risks to information security and regard them as a personal duty. Despite the evidence that the human element plays a major part in the risks, most of operators have relied on electronic protection systems to secure confidentiality, integrity and availability; but this is no longer a safe option. This source of vulnerabilities includes all those human aspects and conditions that an attacker could take advantage of to successfully achieve its malicious objectives. This vulnerability depends on the security training employees receive and the security actions taken by organisations, especially regarding the use of network communications and the management and configuration of the smart grid assets in order to ensure that their communications are done securely and reliably.

According to the document *Smart Grid Security*[20], attacks could be classified into three main categories depending on the target to attack:

- Component-wise attacks target field components that have Remote Terminal Units.
- Protocol-wise attacks are focused on the communication protocol (reverse engineering, false data injections).
- Topology-wise attacks target the topology of the network by carrying out Denial-of-Service.

4.3 Sample attacks against Smart grid communication networks and learnt lessons

The previously listed vulnerabilities and risks could be exploited by attackers with different motivations and could cause different levels of damage and cascade effects to Smart grids. This section includes examples about real life attacks against Smart grid communication networks and learnt lessons. Most of them have been obtained from the information gathered from the interviews made with experts who contributed to this document (see Figure 7). For more detailed scenarios and attack cases, please see "*Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping*"[23] and TACIT framework for the assessment of risk and impact of cyber-attacks in smart-grids[24].

Figure 7: Sample Smart grid attacks.

TARGET ELEMENT	ATTACKS	LEARNT LESSONS
Attack in Control Centre System	One of the worst scenarios considered included an attack to the Control Centre system. Due to a Distributed Denial of Service (DDoS) attack or malware infection, communications and control	Network segmentation:

[23] NESCOR. "Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping", 2014.
[24] Threat Assessment framework for Critical Infrastructures proTection http://www.tacit-project.eu/content/home

TARGET ELEMENT	ATTACKS	LEARNT LESSONS
	of the network was lost, causing an energy production halt. This could affect several systems in different countries.	• Provides privacy and isolation between different system groups; • Protects devices and provides network redundancy.
Data theft	Another scenario considered a data theft, where technical information regarding internal workings and operations was leaked. This could be caused by malware on the computers, due to users having too many permissions or the use of weak encryption or authentication protocols.	• Disable unnecessary services and ports; • Implement secure protocols; • Use stronger encryption; • Optimize of data traffic (only necessary data).
FTP server attack	This attack is carried out by using brute force to obtain user access. The attackers broke the password and obtained access, but this did not have any relevant impact.	• Use robust and strong authentication and encryption methods. • Furthermore, the use of Secure FTP variants is recommended in order to avoid sending clear-text passwords throughout the network.
Man-in-the-Middle attacks (MITM)	Alter the communication between two network components which are communicating directly. This process frequently consists on monitoring the network, intercepting data transferred and using brute-force decryption.	Public key infrastructures (PKI) can be used in order to: • Provide mutual authentication (using secret keys and passwords); • Monitor cryptographic hash function (latency); • Detect possible MITM attacks.
Internal employee incidents	This includes employees, contractors or external users, which can potentially damage an organization from the inside. Their motive can be varied, including revenge, monetary gain, or espionage. In addition, employees who are ill-prepared could unknowingly become a security risk.	• Implementation of an access control and monitoring system capable of detecting these types of incidents. • Provide training and awareness courses to inform users of these risks.
Lack of Standardization	There is a lack of common standards about the security of devices on a Smart grid. In addition, there are too many devices, considerably dispersed. The consequences of this lack of standardization include an increase of the vulnerabilities that could be exploited.	The main objective is to define a standard (such as NERC CIP) that covers the security vulnerabilities that affect these devices (user privileges, data analysis, protection, etc.).
Electric Vehicle vulnerable connections	Electric Vehicles require additional connections in order to exchange the necessary data for its proper operation. These connections use well known protocols by attackers (such as Bluetooth, Wi-Fi or GPRS).	Experts are working on solutions to these risks, analysing new protocols and interfaces used, and defining the appropriate security measures to protect them.
Social engineering	Social engineering attacks (e.g. Phishing) have increased exponentially these last years, and have become one of the biggest concerns for security experts. These attacks focus on the personnel and their aim is to steal operational or business data, user credentials, private data, etc.	• One the biggest concerns relates to internal threats. Organizations should ensure that their employees are aware of the threats they face in order to maintain a good level of security. • Awareness campaigns can be used to train employees.
DDoS and blackouts	The risk of external disruptive events always exists (natural disasters, malicious attacks, etc.) and will impair or disrupt the ability to supply electrical energy and could damage the control	The major challenge with these situations is trying to prevent them and improve existing mitigation measures and service restoration

TARGET ELEMENT	ATTACKS	LEARNT LESSONS
	systems. Most of DDoS attacks consist on overflowing these systems with traffic from multiple sources.	plans. For example, getting more redundant systems to avoid communication blackouts.
Authentication (encryption, weak level)	These weaknesses could potentially be exploited by an attacker in order to gain access to the system or to internal data. These situations could act as a previous step for more elaborate attacks (system damage, information theft, blackouts, etc.).	• The physical protection of metering devices should be robust. • Electric metering devices now have the computational power needed to implement cryptographic measures, although this is not always done.

5. Security good practices in communication networks for Smart grids

This chapter presents a gap analysis to evaluate which areas require further revision, as well as detecting those constraints, impairments and incentives that can affect the development and implementation of smart grid technologies on the different power grid domains. Furthermore, a summary of the good practices that can be applied to Smart Grid communication networks is defined.

5.1 Common security practices currently used by European smart grid operators

This section focuses on presenting the most common security practices that are carried out by smart grid operators located within the European Member States regarding communication networks. Regarding the overall security for smart grids, ENISA already published the report "*Appropriate security measures for smart grids*"[25], in order to help smart grid providers to improve the security and the resilience of their infrastructures and services. This technical document provides guidance to smart grid stakeholders by providing a set of minimum security measures which might help in improving the minimum level of their cyber security services.

Regulations/normative used

The European Commission decided to set up a Task Force on smart grids aiming to develop a common EU smart grid vision and identify key issues that need to be resolved[26]. The Task Force consists of a steering committee and three Expert Groups. The high level steering committee includes regulatory bodies, Transmission Systems Operators (TSOs), Distribution System Operators (DSOs), Distribution Network Operators (DNOs), and consumer and technology suppliers working jointly to facilitate the smart grid and smart metering development. Therefore, there is a conscious effort within Europe to harmonize smart metering/grid standards, and to create a single set of European standards that will be widely adopted. These standards will play a key role to ensure a successful integration. A significant part of this endeavour targets challenges to the new and existing communication architectures, and possible solutions to achieve this integration.

- **Smart metering communication standardization in Europe**: Metering standardization (including automatic/remote meter reading, multiple dynamic tariffs, energy export functions, variable scheduled meter reading and demand control) is a well-established activity in Europe, where various organizations have been formed:
  - ***CEN***: European Committee for Standardization.
  - ***CENELEC***: European Committee for Electro-technical Standardization.
  - ***ETSI***: European Telecommunications Standards Institute.

  Besides communication network standards for smart metering, these organizations also cover important standards for other aspects of smart metering. For example, IEC 61968-9 specifies interfaces for meter reading and control. It specifies the information content of a set of message types that can be used to support many of the business functions related to meter reading and control (e.g. meter reading, meter control, meter events, customer data synchronization and customer switching). It also defines a list of functionalities such as metrology, load control, demand response and relays, as well as a related set of XML-based control messages.
- **Worldwide standardization:** It is worth noting that there are other major smart grid standards worldwide; for example, in the United States the IEEE P2030, IEEE 1547, ANSI, NIST and future IP for smart grids in the IETF have been developed. For instance, it is important to mention the development of the ANSI C12 suite of

[25] ENISA. "Appropriate security measures for smart grids", 2012.
[26] FAN Z. et al. "Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities", *IEEE*, 2013.

standards in the US, which focus mainly on electricity meters. These standards are now being upgraded to reflect advances in smart metering, such as C12.19 Standard for Utility Industry End Device Data Tables (data models and formats for metering data) and the C12.22 Standard for Protocol Specification for Interfacing to Data Communication Networks (communicating smart metering data across a network).

The IEEE P2030 project addresses smart grid interoperability, aiming to provide guidelines for enabling the integration of energy technologies with information and communication technologies (ICT) in order to achieve a seamless operation of the grid components and overall a more reliable and flexible electric power system. The IEEE 1547 Standard outlines a collection of requirements and specifications (performance, operation, testing, safety, and maintenance) to interconnect distributed energy resources with the distribution segment of the electric power system. These are globally needed for the interconnection of distributed energy resources, including distributed generators and energy storage infrastructure, which are essential in order to achieve a successful implementation of smart grids.

ANSI/ISA 99 is a Security Guideline and User Resource for Industrial Automation and Control Systems. It contemplates compliance metrics as a central key issue. Their use can enable a measurement of the increased security level. This in turn might lead to an implementation of cyber-security standards that are not cost related.

NIST is responsible for developing information security standards and guidelines, including minimum requirements for US federal information systems. It is a solid reference for industrial and business organizations. It has also developed an elaborated framework where specific controls are provided for a broad number of areas, sorted depending on the impact they have on the considered information systems. NIST 800-53 includes an Appendix where this control framework has been adapted to the ICS requirements, both by updating existing controls and by adding new ones.

IEC TC57 WG15 has developed cybersecurity standards for power system communications, specifically the IEC 60870-5 series, the IEC 60870-6 series, the IEC 61850 series, the IEC 61970 series, and the IEC 61968 series. The IEC 62351 standards (some under development or update) consist of:

- *IEC/TS 62351-3*: Security for profiles including TCP/IP.
- *IEC/TS 62351-4*: Security for profiles including MMS.
- *IEC/TS 62351-5:* Security for IEC 60870-5 and derivatives.
- *IEC/TS 62351-6*: Security for IEC 61850 profiles.
- *IEC/TS 62351-7*: Objects for Network Management.
- *IEC/TS 62351-8*: Role-Based Access Control.
- *IEC/TS 62351-9*: Key Management.
- *IEC/TS 62351-10*: Security Architecture.
- *IEC/TS 62351-11*: Security for XML Files.
- *IEC/TR 62351-12*: Resilience and Security Recommendations for Power Systems with DER - under development.

- **Other relevant standards:** ISO 27001[27] is considered as a mature, general purpose standard that provides good practices and recommendations for information security management and is normally used for the implementation or management of Information Security Management Systems (ISMS). As information security is a general concept that affects all sectors and areas, it applies to all branches of an organization (not only specific security systems or SCADA systems). Its application should be appropriate for smart grids and SCADA systems.

[27] FINARDI U. et al. "Considerations on the implementation of SCADA standards on critical infrastructures of power grids", *CNR Ceris*, 2013.

- ***Common Criteria***[27] is an international standard for computer security certification. It povides assurance that the phases of specification, implementation and evaluation of a computer security product has been conducted in a rigorous, standard and repeatable manner at a level that is proportionate with the target environment for use.
- ***NERC CIP***[27] is closely connected to the reliable operations' support for bulk Electric Systems, providing a cyber-security framework for the identification and protection of Critical Cyber Assets. The current NERC framework recognizes the roles of each entity in the operation of the Bulk Electric System, the criticality and vulnerability of the assets needed to manage Electric System reliability, and the risks to which they are exposed.

Security protocols most used

To deal with potential security threats within the smart grid, countermeasures and defence strategies have to be widely deployed and integrated into both the network protocols and the architectures used. For example, compared with legacy power systems, the smart grid features full-fledged communication protocol stacks to accomplish the goal of secure and efficient communications in the entire network.

Recently, as described on "Considerations on the implementation of SCADA standards on critical infrastructures of power grids"[28], many efforts have been made within the power community to develop secure protocols for power grids, most of which are reusing existing protocol suites to achieve secure communications, such as IPsec, Transport Layer Security (TLS) and IPv6[34]. Apart from existing protocol suites, security extensions for power communication protocols have also become a primary focus in the literature and standardization e.g. the security extensions for the two widely-used power grid communication protocols, DNP3 and IEC 61850.

Secure data aggregation protocols have been also proposed for the smart grid, since the bottom-up traffic model (device-to-centre) can be applied in power systems, such as metering reading in the AMI network and device monitoring in the SCADA network.

Design of the smart grids

Physical and logical network architecture designs should limit or isolate the different individual domains that form up the smart grid, leaving only those interconnections needed. For this purpose, normally one of the following two proposed secure smart grid network architectures is used[28]:

- Trust-based computing architecture.
- Role-based network architecture.

Cryptographic primitive based approaches have become one of the major countermeasures applied against attacks that target network integrity and confidentiality and which can be affect the overall performance. The main topics regarding this issue are: encryption, authentication and key management for power systems. Some of the research challenges are:

- Trade-off between security and latency.
- Emerging physical-layer authentication.
- Symmetric key management for time-critical systems.
- Key management for advanced metering infrastructure.

[28] WANG W. & LU Z. "Cyber security in the Smart Grid: Survey and challenges", *Computer Networks*, 2013.

Contracting with network operators

There are not standards or guidelines defined to be used by operators or companies regarding security practices for contracting services to network operators. However, common sense dictates that the following points should be considered:

- Use of Service Level Agreements (SLA) applied by contract in relation to the requirements that the provider has to comply with (such as bandwidth, quality of service, coverage or support).
- Redundancy in network communications.
- Use of different protocols and technologies.
- Contracts with different network operators.

Moreover the following "Evaluation criteria on communication technologies"[29] should be taken into consideration:

Non-technical:

- costs
  - OPEX
  - CAPEX
- operator's authority
- customer acceptance

Technical:

- availability
  - temporal
  - local
  - max. downtime
  - reliability
  - performance
    - data throughput
    - capacity
      - coverage
      - nodes per cell
      - clustering
    - latency
  - physical medium
    - right of use
      - licence free
      - primary /secondary
- internal consumption
- installation efforts
- integrability
  - functional
  - multicasting
  - scalability
  - life span
  - standardization
  - quality of service
  - guaranteed future
  - network-security
  - technology dissemination
  - combinability with other technologies
  - network management
  - operating efforts

[29] Presentation "Challenges Regarding Security & Reliability of the Communications Infrastructure in Smart Grids", Dr. Markus Wächter, 2015

- topology
- distance without repeater

Procurement and certification of the systems

In order to include certification requirements in the procurement process, certifications should focus on the whole life-cycle of the product not only on the product itself; from the initial design phase and up to their end of life. Additionally, a certification scheme will need to incorporate the different types of certifications that apply to the product life-cycle, because product development certification, product certification and operation certification cannot be subject to the same certification type. Currently, the procurement process includes certification requirements which only focus on products like smart meters (i.e. secure protocols, physical security, and cryptography).

Testing the smart grid components

This includes testing all participating components in the smart grid context: system actors, applications, power system equipment (typically located at process and field level), protection and tele-control devices, network infrastructure (wired / wireless communication connections, routers, switches, servers) and any type of computers used. It addresses the security of the individual components, focused on hardware, software, and the functions the devices should perform and support. The process for testing the smart grid components includes conformity testing, functional testing and interoperability testing[30]:

- ***Conformity testing***: assess the compliance of the test subject to standardised requirements.
- ***Functional testing***: assess the ability of the test subject to provide the required functionality. This functionality is usually described in a standard referred to during the tests.
- ***Interoperability testing***: assess the ability of two or more systems to exchange information and to make mutual use of the information that has been exchanged.

A more specific form of testing that is commonly carried out in security audits is penetration testing. This type of testing revolves around the exploitation of possible design flaws and weaknesses to compromise the security of a device. Such tests do not focus on a specific test book, but rely more on the creativity of the tester, and the time that there is available to carry out the test. Penetration testing can be incorporated as part of a functional test, by describing it as a negative test case for a functional requirement. Depending on the nonconformity risks, it can be decided to perform first, second and third party assessments. However, in practice, only third party certification is seen as trustworthy for most cyber security specialists.

5.2 Gap analysis and identification of areas of improvement

The first step is to develop a gap analysis to detect weak areas and possible improvements to the grid's security. According to the results of this analysis the following areas are in need of improvement:

Technical points of attention

There are several domains that require security-related improvements in order to ensure the protection of the grid itself:

- **Last mile awareness as part of cyber-security awareness campaigns**: The logical security measures on the last mile of the network have to be taken into consideration. This part of the network is already protected at physical

[30] ENISA. "Smart Grid Security Certification in Europe: Challenges and recommendations", 2014.

level, but in most cases the cyber security is insufficient or inexistent. Smart grids companies should protect the last-mile communication systems from three dimensions: data, device and communication.

- **Always use secure communication protocols on SCADA devices**: since most SCADA protocols were designed long before network security was considered as a relevant risk, applying security measures on SCADA protocols was not considered as a priority. This however is no longer the case, and secure communication protocols have become a must in order to protect smart grids.
- **Always use interoperable communication protocols on SCADA devices**: SCADA devices designed by different manufacturers used their own proprietary protocols, that in have been compatible with devices produced by same manufacturer. Due to the distributed nature of smart grids, these devices must now be compatible, not only for security but also in order to guarantee the power supply on the grid.
- **Avoid the use of proprietary/homebrew protocols on SCADA systems and other related assets**: related to the previous point, not only must SCADA systems be compatible with each other; it is also highly recommended for them to use standardized protocols defined by the whole industry, not individually by each manufacturer.

Organizational needs in the smart grid domain

Service Providers, Customer and Markets domains need specific and properly defined policies and standards covering all smart grid domains and areas (communications, billing, customer management, account management, installation and maintenance, micro generation, etc.). There are several possible steps for improvement:

- **Develop policies to ensure periodic software and firmware updates to SCADA systems**: as these systems are now interconnected, and in many occasions passing through the Internet and other public networks, it becomes necessary to update them periodically to fix vulnerabilities and add new security measures to ensure the safety of the smart grid communications.
- **Foster guidelines regarding smart grid communications officially supported by all MS**: the Member States' competent authorities should harmonize policies regarding the security of smart grid communications in order to standardize them and ensure a smooth implementation of smart grids in different environments.
- **Involve vendors and manufacturers in the protection of the devices and network elements**: Vendors and manufactures are not sufficiently involved in the security development process of the smart grid devices, which is required in order to implement the security measures by default on them. For this purpose, it will be necessary to establish common regulatory bodies in Europe in charge of establishing a baseline containing a set of basic features that all manufacturers should always implement on their products.
- **Cybersecurity awareness campaigns for smart grid company employees**: Security incidents could be more easily avoided if employees are aware of these risks and are prepared against them. For this purpose it is necessary to offer them awareness campaigns in these topics.

Certifications needed specifically for smart grid security

There are many defined standards for different aspects of the protocols, architectures and smart grid devices. However there is a lack of alignment in these guidelines, as there is no preferred one, and nowadays manufacturers and vendors can make use of any of them without any regard about the one used by the rest. This leads to compatibility problems, especially on the intercommunications and interdependencies between devices, leading to further problems later on during the deployment of the smart grids. Therefore, the lack of standardized certification schemes at a European level is a problem that must be worked on and solved in order to improve greatly the security and efficiency of smart grids.

Issues highlight during the interviews

During the interviews it was underlined the lack of studies regarding interdependencies among smart grid devices and their intercommunications between the grid implementations of the different European Member States. This

lack of knowledge leads to the need to further evaluate them in the future. This specifically refers to each individual implementation, and as such each individual case would have to be evaluated. However, it is still highly recommended to establish a common baseline throughout Europe in order to avoid current and future interdependency issues among Member States' smart grids.

5.3 Constraint and incentive analysis for the deployment of security measures

The constraints, impairments and incentives that affect the security measure deployment process on smart grids can be divided into four mayor groups:

Economic constraints and incentives

Fragmented markets are the main barrier that impedes the smart grid implementation process. Due to the lack of a harmonized approach, implementation costs rise considerably. Still, there are similarities among countries that can be used to create consensus, and a combination of schemes could be an acceptable solution on a European level, which would also impact in lower costs. It will be a challenge to keep cost to a minimum level while still providing enough security; as security is a topic that penetrates all aspects of a system, and therefore has to be widely implemented without directly providing justification of the necessary costs and effort. The benefits of the implementation of security measures are shared among different groups[31]: such as the firms operating in the country or the society as a whole, and only a small part concerns the electricity utilities. From a profitability viewpoint, electric companies have no direct incentive to increase their security levels, as cyber-threats have been irrelevant to legacy power grids until the arrival of smart grids. This explains their reluctance to perform such huge investments. Public regulation and support to firms operating in competitive branches of the energy sector is definitely necessary. Electric supply security is a very important point of the electric service, since our lives and economic activities have become more and more dependent on this commodity, and a lack of supply would cause huge losses and overall panic. Technical security measures are usually quite expensive to implement (e.g. communication network redundancy cost-effective system, security requirements implementation by manufacturers, etc.), and as such need their cost-effectiveness needs to be evaluated in each case.

Organizational constraints and incentives

Heterogeneity and differences in applicable regulations on the European Member States countries are one of the main concerns in this case. In particular:

- Different national regulations, although a common framework established by the UE already exists.
- Different roles of public firms.
- Different national market structures.

Cyber-security is not currently at the front-line, as not enough attention is being paid in Europe to cyber-security and data privacy protection. There is a generalized perception that cyber-security is not a critical aspect of the smart grids. Furthermore, the governments of several European countries are rushing to develop and deploy their smart grids. Unfortunately, rushing at this point can be counter-productive, causing the resulting infrastructure to lack the appropriate security measures. However, the benefits of having aligned standards and recommendations outweigh its costs. By having the same standards, all European countries will implement their own smart grids following similar architectures and trends, helping greatly to ensure the compatibility and proper interdependency and intercommunication of all their systems and services.

[31] GARCÍA GUTIÉRREZ F. and RAGAZZI E. "Trial evaluation: conclusive lessons from Essence case studies", Rapporto tecnico N.42, 2014

Technical constraints and incentives

There is a lack of standard reference architectures for smart grids in Europe. There are many standards, but no single one is considered as the baseline for implementations of these networks, independently of the domain evaluated (including generation, distribution, transmission and customer premises). For technically-complex devices, their configuration and management is difficult, especially in implementations with large number of devices. Therefore this increases the cost of applying new configurations or updates on them in order to fix vulnerabilities. Manufacturers have to design their devices in a way that they support easier upgrade and management solutions. This also applies to large intercommunication networks, where their management and protection also requires large investments. Therefore, while the implementation of security measures is costly, and has considerable technical implications, its benefit is clear as their protection, and of their interdependencies, ensures the proper operation and working of the grid and their systems, allowing for more efficient energy distribution and taking advantage of all the new features and services that smart grid support

Social constraints and incentives

Smart grids can be considered as critical infrastructures, as they are essential in order to maintain vital societal functions, health & safety and economic status of the people. The disruption or destruction of such infrastructures could have a serious impact on a Member State, which leads to the need to protect them. This is even more applicable for the intercommunication networks and interconnections in smart grids, as an attack on them can have the same nefarious effect as a physical attack against the traditional power infrastructure. Unfortunately, security awareness and public perceptions on these risks are still low, and requires a lot of work to be changed; for this purpose, it is recommended to include awareness campaigns on the long term deployment plans in order to ensure that they are informed and aware of these new needs.

5.4 Available communication security guidelines applicable to Smart grids

There are various good practices published for all aspects of communication networks, communication devices, Smart grid systems and SCADA devices. This section is focused on summarizing those that are relevant to this study, which mainly concerns those regarding Smart grid devices and architectures, and communication networks in general.

The documents that have been considered as part of this section are:

- Best practices for handling smart grid cyber security[32].
- Connecting and securing Legacy Electrical substations to the smart grid[33].
- ENISA Good Practices in Resilient Internet Interconnection[34].
- ENISA Recommendations for Europe and Member States[35].
- NESCOR Electric Sector Failure Scenarios Common Vulnerabilities and Mitigations Mapping.
- Smart Grid Security: Threats, Vulnerabilities and Solutions[20].
- ENISA Smart Grid Threat Landscape and Good Practice Guide[21].
- ENISA Threat Landscape and Good Practice Guide for Internet Infrastructure[25].
- NIST Guidelines for Smart Grid Cybersecurity[36].

[32] GHANSAH I. "Best Practices for Handling Smart Grid Cyber Security", *California State University Sacramento*, 2014.
[33] MACKENZIE H. "Connecting and Securing Legacy Electrical. Substations to the Smart Grid", *Belden*, 2015.
[34] ENISA. "Good Practices in Resilient Internet Interconnection", 2012.
[35] ENISA "Recommendations for Europe and Member States", 2012.
[36] NIST. "Guidelines for Smart Grid Cyber Security", 2010.

- OSCE Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace[37].

Figure 8 displays a list of these categories, with the good practices that apply to each one. These good practices have been numbered in order to better reference them throughout the document.

Figure 8: Good practices.

CATEGORY	GOOD PRACTICES	ASSOCIATED ATTACKS
Organizational security policies (smart grid communications)	**GP01 - Organisational security framework Implementation**: describes the implementation process of the security plans.	Attack in Control Centre System, Data Theft, Authentication exploiting
	GP02 - Password policy: it is necessary to establish a strong and robust password policy. This can sometimes require employee training regarding how to choose robust passwords and their impact in their work processes. Awareness against social engineering is also recommended on this point.	
	GP03 - Data Policy: data must be classified according to their security level, which has to be applied throughout the whole lifecycle of the data up to the point where is destroyed. The classification levels have to be clearly defined as part of the corporate security policy.	
	GP04 - Incident Response: it is necessary to define the process to manage security incidents. This includes all stages: detection, investigation, analysis, mitigation, disaster recovery (business continuity plans), and post evaluation (define measures to prevent future incidents).	All attacks (faster detection and mitigation)
	GP05 - Relations with compatible providers: communication channels between providers and other third parties can be used to receive assistance and share relevant information to prevent large-scale incidents or attacks.	
Annual assessments	**GP06 - Vulnerability assessments in communication networks**: vulnerability assessments should be carried out annually for all critical elements of the smart grid networks to verify their security level and detect any possible vulnerability. Non-critical devices should still be assessed, although that need not be done annually.	Exploit attacks to outdated elements
Security by Design	**GP07 - Security by Design**: security considerations need to be included on the initial phases of the smart grid design, to ensure better compatibility. Failure to do this will most likely lead to much higher implementation costs.	All attacks
Mutual authentication	**GP08 - Mutual authentication**: the origin and destination of all communications must be known. By using mutual authentication, both the server and the host verify each other's identity. This is usually done using TLS or IPsec protocols, or by implementing a Public Key Infrastructure (PKI).	MITM, Information theft, identity spoofing
Virtual private network	**GP09 - Virtual Private Networks**: these networks should be used to establish a connection within two devices on the communications' architecture. These connections establish a secure point-to-point communication through the network by using tunnelling and encryption protocols. It is especially recommended as a means of connecting remotely to a system.	MITM, Eavesdropping, information theft
Third-party companies	**GP10 - Communication service providers**: utilities are not used to manage large complex communication networks, as their focus is the power grid. For this purpose, it is recommended to make use of third party telecommunication companies that will be in charge of maintaining and securing the network communications.	DoS, DNS attacks, unauthorized access
	GP11 - Supply Chain Management: system security is only as strong as its weakest link; therefore when working with third-party providers, it is fundamental to define a management process to ensure that all security requirements are met.	Social Engineering,

[37] OSCE. "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace", *OSCE Publications*, 2013.

		information theft
Physical security	**GP12 - Physical access rules**: physical access to the elements of the network must be restricted; personnel must only have access to those systems/infrastructures specifically required.	Unauthorized physical access, information theft, deliberate damage
	GP13 - SCADA networks: periodical surveys to verify the physical security of the remote sites connected to the SCADA network.	Unauthorized physical access, deliberate damage
Software updates	**GP14 - Software updates**: an update process that ensures that all the elements of the network are up-to-date and protected against newly discovered vulnerabilities or bugs should be established.	Attacks related to exploit outdated systems (Data Theft, DDoS…)
Network Intrusion Detection/Prevention Systems (IDS/IPS)	**GP15 - Advanced IDS modes:** the use of host-based defence mode and of Domain Specific IDS is highly recommended to boost the security of the network, especially of the most sensitive segments. As this cannot be always achieved, it is recommended to complement it by including a baseline of the operations and expected flows to detect any anomalies.	Unauthorized access, information theft, malicious code
	GP16 - System unification: to improve the defence of the network, it is highly recommended to unite all IDS/IPS systems in one "group", allowing operators to gain comprehensive situational awareness. This approach is more comprehensive in terms of security and event monitoring, and provides better protection for the overall network.	
Employee awareness, training and education	**GP17 - Employee awareness, training, and education**: employee awareness is fundamental in order to prevent attacks and fraud. Teaching employees to detect attack patterns, risks, fraud and social engineering attacks. It is recommended to include this point as part as the corporate security policy and carry out periodical awareness campaigns.	Social Engineering
Contingency readiness	**GP18 - n-1 contingency**: the system should be distributed in a way that a failure of one device will not cause a communications outage in a section of the network. This can be achieved with redundant communication devices that ensure that no device is connected only through one path.	Denial of Service Attack, Outages
Malware protection	**GP19 - Manufacturer code and software validation**: systems should only run the intended functions and applications they were designed to. Manufacturers should provide means to validate the software and firmware installed on the system.	Unauthorized access, information theft, malicious code
Secure network segregation	**GP20 - Network segmentation**: the network should be divided into sections, each one for different purposes, to protect the systems within. This allows the protection of especially sensitive network components, such as the AMI segment or the control systems segment. This helps to limit unauthorized accesses to one segment to gain access to other sections of the network.	Unauthorized access, malicious code, network outage cascade effect
	GP21 - Network assets as segregation elements: network segments have to be separated with security devices, including firewalls, gateways and filtering routers, to stop users from one segment to access other segments, except if they are specifically allowed.	
	GP22 - Use of firewalls and Demilitarized Zones (DMZs): limits within the internal network segments and the DMZs should be separated though the use of security devices (e.g. firewalls). These firewalls should be protocol-aware, including support for basic filtering of both protocols and command codes/instructions.	
Secure network communications	**GP23 - Secure smart device communication**: smart grid information systems should only make use of secure communication protocols (such as SSL/TLS). Additional security measures can be taken in order to further protect these communications.	Information theft, MIT, identity theft,

	GP24 - Secure communications used for remote administration: remote management and administration of the smart network systems must always be done though secure communications or VPNs connections.	deliberate information manipulation
	GP25 - Protocol compliance: communications though the network should only use protocols approved by the provider and which have been verified to work on the network and have security capabilities.	
	GP26 - External smart grid information systems: their communications should be always identified and protected to avoid corruption, tampering or loss.	
	GP27 - Access control points: Smart grid information system routes all remote accesses through a limited number of managed access control points.	
	GP28 - Only use authorized communication channels: communication and information flows should be defined and limited over the communication link.	
	GP29 - Secure network proxies: internal and external network connections should be routed via specifically hardened proxies, located on the DMZ.	
	GP30 - CSP redundancy: avoid depending on a single CSP, instead make use of several different ones.	
	GP31 - Secure communication protocols: In order to protect communications, it is necessary to use secure protocols.	
SCADA security	**GP32 - Smart SCADA audits**: technical audits on SCADA devices and networks should be carried out regularly. The focus is to detect vulnerabilities and analyse them to determine the risk level they pose. This includes managing and overviewing the application of corrective actions.	Information theft, MIT, identity theft, deliberate information manipulation
	GP33 - SCADA connections knowledge: it is necessary to build up a knowledge base of the SCADA networks and the devices contained in order to be able to evaluate their strength, detect possible improvement points and develop recovery plans.	
	GP34 - Disconnect unnecessary connections to the SCADA network: disconnect or isolate SCADA network devices and the SCADA network itself from the rest of devices. DMZ areas can be used for this purpose in various architectures.	
	GP35 - SCADA backdoor management: any backdoor access to the SCADA network should be closed unless strictly necessary. If it is not possible to close it, additional security measures should be taken in order to protect it as much as possible and avoid any potential derived risks.	
	GP36 - MTUs & RTUs: these devices should be protected, using Secure Architecture Designs and applying security features provided by the devices, as well as implementing IEC-60870, DNP 3.0 and Modbus protocols.	
Wireless Area Networks	**GP37 - Wireless networks**: the following security measures can be used to protect networks in general (including Wi-Fi, ZigBee, WiMAX): • Media Access Control (MAC) address filtering; • AES encryption protocols; • Protection against masquerading parties; • Access Control Lists (ACL); • Trust Centre address configuration (ZigBee only); • IEEE 802.11w-2009 and WPA (Wi-Fi only).	Information theft, MITM, identity theft, session hijacking, information gathering
Advanced Metering Infrastructure	**GP38 - Metering security standards**: adopt an open-reference standard that defines the security measures that advanced meters should comply with.	Smart Meter hijacking, information theft, malicious code, unauthorized access
	GP39 - Traffic control: implement session control and detection mechanisms capable of quickly halting any suspicious sessions or communications.	
	GP40 - Network connection only for approved assets: authenticate and validate the identity of the metering assets on the network and restrict access to any unknown device. This authentication is also used to provide data integrity.	

	GP41 - Authentication and integrity checks: validate and authenticate the origin of all system commands and meter readings to ensure that they have not been tampered with. Configurable firmware is the most vulnerable if these security checks are not carried out.	
	GP42 - Meter data encryption: this protects the data against tampering and ensures the privacy of any personal data transmitted.	
	GP43 - Consumer non-repudiation: provide means to ensure that any data obtained is valid and its origin has been verified.	
	GP44 - Virtual Home command execution: all commands received from external sources should be tested firs in a "Virtual Home Command Execution" environment (a form of sandbox), to ensure that no negative effects occur from its application on the real environment.	
	GP45 - Head-end: possible security measures to implement are: • Authenticate all commands and reports between the Head-End and the customer endpoint. • Protect the Head-End systems with the same level of security as other critical assets. • Use strong user authentication on all Head-End systems and log all user actions. • Implement safety logic to prevent rapid changes in pricing information. • Carry out periodic integrity checks and audits.	
Denial of Service protection	**GP46 - IP address verification**: source IP addresses should always be verified, especially on those systems located on the edge of the Internet infrastructure, to prevent address spoofing.	Denial of Service attacks, communication network outage, DNS attacks
	GP47 - DNS issues: name-server operators should implement measures, such as RRL, to protect against vulnerabilities that can be used to compromise the organizations' network.	
	GP48 - Denial of Service protection: anti-DDoS systems should be established to protect AMI systems and protect other devices on the network against Denial of Service and replay attacks.	
Asset management	**GP49 - Asset inventory**: an inventory containing all the assets and devices part of the network should be created and maintained in order to gain awareness of the whole network, avoiding missing any system or obscured/legacy section. Furthermore, this inventory should contain the vulnerabilities that affect each one in order to determine risks and possible threats to the network.	Unauthorized access, malicious code, network outage

5.5 Categorization of good practices on smart grid communication networks

After the study of existing good practices, and sorting them into relevant categories, the next step is to evaluate and organize them based on their impact, focused on people, technical and organisational aspects. The concepts evaluated are:

- **Smart grid domains** are related to: people, organizational aspects or technical aspects.
- **Implementation complexity**: rate their implementation difficulty based on the requirements related to the domains defined previously. The ratings go from "low" (feasible) to "high"(not feasible).
- **Cause**: justification of the rating given to the implementation complexity column.

The table on Figure 9 presents the result of the evaluation carried out following the specifications defined for the analysis.

Figure 9: Good practices by domain.

SMART GRID DOMAIN	GOOD PRACTICES	IMPLEMENTATION COMPLEXITY	CAUSE (ECONOMICAL, TECHNICAL OR POLITICAL)

People	GP17 - Employee Awareness, Training and Education	LOW	**Economical**: use of internal/external resources in order to enhance personnel security awareness.
Organizational aspects	GP01 - Organisational security framework Implementation	LOW	**Economical**: use additional resources in order to implement the security plan on the organization.
	GP02 - Password policy	LOW	**Technical**: enforce the correct password policy in both systems and devices.
	GP03 - Data Policy	LOW	**Political**: national or European Regulation regarding data protection must be enforced.
	GP04 - Incident Response	LOW	**Organisational**: elaborate and implement an incident management and response plan.
	GP05 - Relations with compatible providers	MEDIUM	**Organisational**: collaborate with providers and suppliers regarding incidents.
	GP06 - Vulnerability assessments in communication networks	HIGH	**Economical**: use internal/external resources in order to test security resiliency.
	GP10 - Communication service providers	MEDIUM	**Economical**: cost of contracting communication services to third party providers.
	GP11 - Supply Chain Management	MEDIUM	**Organisational**: establish security requirements to suppliers and the contracted processes.
	GP12 - Physical access rules	LOW	**Organisational**: define access rules according to the job requirements of the personnel.
	GP13 - SCADA networks	MEDIUM	**Economical**: test the physical security resiliency of the SCADA networks.
	GP18 - n-1 contingency	HIGH	**Economical**: deploy redundant network installations for transmission grid.
	GP49 - Asset inventory	MEDIUM	**Technical**: lack of knowledge of the assets within the network may complicate their securitization.
Technical aspects	GP07 - Security by Design	LOW	**Technical**: hardware and network security awareness for designers.
	GP08 - Mutual authentication	MEDIUM	**Technical**: authenticate both ends of the communication to verify their identity.
	GP09 - Virtual Private Networks	MEDIUM	**Technical**: design and implement security measures to the VPN connections to the network.
	GP14 - Software updates	HIGH	**Technical**: defining and implementing an update process can be complex for real-time assets.
	GP15 - Advanced IDS modes	MEDIUM	**Economical**: cost of deploying network defence measures on the network infrastructure.
	GP16 - System unification	MEDIUM	**Technical** and **organizational**: design and implementation costs, including the need of collaboration between different companies.
	GP45 - Head-End systems in Advanced Meter Infrastructure	MEDIUM	**Technical**: integration of the Head-End systems on the AMI infrastructure, adaptation of the system and application of new configuration.
	GP19 - Manufacturer code and software validation	HIGH	**Technical**: implement code execution validation controls on the embedded systems.
	GP20 - Network segmentation	MEDIUM	**Technical**: design and implement network segregation. Carry out test to verify connections.

GP21 - Network assets as segregation elements	MEDIUM	**Technical**: device configuration to work with the network segments. Implement firewall rules.
GP22 - Use of firewalls and Demilitarized Zones (DMZs)	MEDIUM	**Technical**: implement and configure firewalls to separate the DMZ of the rest of the network.
GP23 - Secure smart device communication	HIGH	**Technical**: update communication infrastructure to secure SCADA communications.
GP24 - Secure communications used for remote administration	MEDIUM	**Technical**: implement security measures to secure and protect remote communications.
GP25 - Protocol compliance	HIGH	**Technical**: protocols use for intercommunication must comply with applicable security standards.
GP26 - External smart grid information systems	HIGH	**Technical**: implement security measures to all external communications.
GP27 - Access control points	LOW	**Technical**: define needed access control points and limit all these not required.
GP28 - Only use authorized communication channels	MEDIUM	**Technical**: implement measures to ensure that only authorized channels are used.
GP29 - Secure network proxies	MEDIUM	**Technical**: implement and maintain network proxies on the network.
GP30 - CSP redundancy	MEDIUM	**Economical**: cost of maintaining contracts with several independent CSPs.
GP31 - Secure communication protocols	MEDIUM	**Technical**: implement and deploy secure protocols over the whole infrastructure.
GP32 - Smart SCADA audits	HIGH	**Economical**: cost of implementing periodical audits of the SCADA devices and infrastructure.
GP33 - SCADA connections knowledge	MEDIUM	**Organisational**: obtain or train personnel with knowledge on SCADA networks and devices.
GP34- Disconnect unnecessary connections to the SCADA network	MEDIUM	**Technical**: implement and use only those SCADA network devices needed.
GP35 - SCADA backdoor management	MEDIUM	**Technical**: disable unneeded backdoors. Those required will need to be protected.
GP36 - MTUs & RTUs	MEDIUM	**Technical**: deploy security measures to the RTUs and MTUs.
GP37 - Wireless networks	MEDIUM	**Technical**: implement security measures to protect Wi-Fi Communications.
GP38 - Metering Security standards	MEDIUM	**Technical**: comply with applicable standards.
GP39 - Traffic Control	HIGH	**Technical**: implement traffic control mechanisms on the AMI infrastructure.
GP40 - Network connection only for approved assets	MEDIUM	**Technical**: configure network to restrict access to any device not specifically approved.
GP41 - Authentication and integrity checks	HIGH	**Technical**: implement authentication and integrity checks on all devices on the network.
GP42 - Meter data encryption	MEDIUM	**Technical**: implement encryption protocols to protect consumer data.
GP43 - Consumer non-repudiation	MEDIUM	**Technical**: implement non-repudiation mechanisms on the AMI infrastructure.

	GP44 - Virtual Home command execution	MEDIUM	**Technical**: deploy virtual home environment for testing commands before sending them.
	GP45 - Head-end	HIGH	**Technical**: implement protection measures to the Head-End systems of the AMI infrastructure.
	GP46 - IP address verification	MEDIUM	**Technical**: implement fraud detection systems to detect unauthorized or suspicious IP addresses.
	GP47 - DNS issues	MEDIUM	**Technical**: configure DNS to protect against known vulnerabilities and attacks.
	GP48 - Denial of Service protection	HIGH	**Technical**: implement anti-DDoS security measures on the AMI network.

6. Recommendations to improve security of communication networks in smart grids

This chapter presents a series of recommendations to improve the security level of the communication networks used for intercommunications in smart grids. These recommendations are intended mainly for operators, vendors, manufacturers and security tool providers located within European Member States.

The first recommendation will serve as an overview of the rest of recommendations, as a means of establishing the appropriate focus for them.

Recommendation 1: European Commission should ensure the alignment of policy approaches across EU countries to establish a common posture for smart grid communication interdependencies. Cyber security has become one of the main concerns regarding the implementation of smart grids, and especially regarding the networks used for the interconnection of all the assets that make up this new grid. Therefore, an inherent requirement is to protect these communication networks, the data that travels through them and the devices connected to them. For this reason, it is necessary to collaborate with all involved parties (operators, manufacturers, vendors, distributors and security experts) in order to further develop solutions to fill these requirements. Each European country has a different regulation and infrastructure regarding power grids, in many cases due to the specific needs of each one. Furthermore, they tend to make use of different standards for these implementations, architectures and assets in use. European Commission should promote and support initiatives regarding the improvement of smart grid intercommunications security according to the recommendations described on this document, which will serve as a prerequisite to raise the level of smart grid security on both European and National intercommunication networks. There is the need to harmonize European requirements and standards for smart grid communication networks, especially regarding the homologation of security devices and protocols.

Recommendation 2: Manufacturers and vendors should foster intercommunication protocol compatibility between devices from different manufacturers and vendors. Currently, many manufacturers and vendors, due to the lack of standards, make use of their own proprietary protocols and communication systems for the intercommunication between their devices. Therefore, this leads to the fact that when a distributor or utility makes use of these devices, the rest of the network devices have to be provided by the same vendor, or have to be specifically compatible with them. This, although can be seen as a benefit from the manufacturers' side, is in fact a grave problem due to the massive size of the smart grid networks, and the fact that many of the devices currently in use come from different manufacturers as different specifications are needed for each network segment. Distributors, utilities and other involved actors should make use of devices from different vendors without having to worry about incompatibilities in the communications among them. Alternatively, providers could make their protocols open-source instead of proprietary, to enable other companies to make their devices compatible with these communications. This has as an additional advantage the fact that by being open source, their implementation can be reviewed by third parties, which can analyze it and find and fix bug and security vulnerabilities.

Recommendation 3: European smart grid operators and relevant authorities should develop a set of minimum security requirements to be applied in all communication interdependencies in smart grids. The first step for improving security of the intercommunications, interdependencies and devices part of the smart grids is to establish a series of minimum security requirements that have to be met in order to protect the overall grid connectivity. These security requirements and associated controls must be defined in order to achieve a minimum level of security that will ensure service continuity and resilience, both in public and private environments. This has to be promoted at a European level in order to ensure its success. This could be done by establishing a working group at a European level, with representation of all relevant stakeholders, in order to define a series of recommendations regarding the minimum security requirements that should always be applied to smart grid devices, intercommunications and

interdependencies. Alternatively, define guidelines that include the implementation of minimum security requirements for all devices, interconnections and interdependencies for the deployment of new smart grids.

Recommendation 4: Manufacturers, vendors and asset owners should implement security measures on all devices and protocols that are part, or make use of the smart grid communication network. Traditionally, grid devices and assets were usually isolated, or interconnected through private local networks. However, smart grids bring a new level of interconnection, where devices can be connected to large networks, wireless networks and even the Internet. This leads to the need to protect these communications against eavesdropping and tampering, from the origin and up to the destination. For this purpose, security measures need to be applied to the devices and the protocols used for interconnection, and this needs to be considered from the device design phase onwards in order to avoid the implementation costs from skyrocketing. This could be achieved by:

- Supporting the implementation of security measures by default on all the protocols used for intercommunications within the smart grid network.
- Boosting the implementation of standard security measures by default on all devices that are going to be part of the smart grid communication network.
- Involving manufacturers, vendors and security tool providers in the process for improving security of both devices and protocols.

Recommendation 5: Manufacturers, vendors and asset owners should work together on updatable devices and periodic security update support. Nowadays, it is the norm for software and firmware to receive periodic updates to fix vulnerabilities, add new security features or fixes, and even add new characteristics. This is quite common on personal devices and servers, where it has become a common practice to establish a periodic update and maintenance phase to ensure that all systems are always up to date. However, the same cannot be said with smart devices in traditional grids, and which now translates to smart grids. Firstly, power grid devices where usually isolated and protected behind physical security measures, and as such it was not needed to update them unless if there was a critical bug. Furthermore, these devices are normally running non-stop 24x7x365, and stopping them requires a considerable amount of time and resources. Devices must be designed to be easily updated, both their software and firmware, in order to ensure that they maintain an acceptable security level. There is no direct alternative in this case as the devices will be interconnected to the main smart grid network, and sometimes even to the Internet, and any security vulnerability found in them has to be fixed. Although it is possible to that in some cases these vulnerabilities can be fixed by applying specific configuration or mitigation features, not all vulnerabilities can be fixed this way. Manufacturers and vendors should work together on this topic, as they need to design their devices to be easily updatable, and need to develop an update program to maintain them updated.

Recommendation 6: European Commission, Member States and all relevant smart grid stakeholders should promote incident reporting and attack patterns sharing. Attacks against electrical grids have not been very common in the past, as many systems where isolated and gaining access to one did not grant an entry point to the rest of the system. However, with the implementation of smart grids, many new attack vectors and network entry points have appeared as a consequence of their intercommunicated and distributed nature. Even more, it is just a matter of time that large attacks focus on them and begin threatening their stability. For this reason, it becomes necessary to share data and attack patterns to help all involved agents to protect their assets and develop countermeasures which can, in turn, be shared to protect the overall smart grid network. This can be achieved by facilitating incident reporting intercommunications to share attack patterns and trends among European agencies, Member State agencies and other relevant stakeholders. Foster attack data sharing between companies and involved stakeholders to prevent future attacks. Establish sharing mechanisms among organizations and countries in order to share data related to attacks suffered, threats and attack trends.

Recommendation 7: European Commission, Member States and all relevant smart grid stakeholders should promote increased training and awareness campaigns. One of the gripes that threats smart grids is also the lack of

qualified professionals, and many of the existing ones lacking adequate training and awareness regarding security in the new scenarios that have appeared on energy grids due to the new features that come with the implementation of smart grid technologies. There are a number of actions that could be put in places:

- Specific training courses to teach operators and manufacturers to implement security measures and to mitigate risks that are inherently part of the smart grid systems.
- Awareness campaigns to inform professionals about the latest threats and risks that affect smart grids and related technologies, as well as possible solution or mitigation actions.

ENISA

European Union Agency for Network
and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office

1 Vass. Sofias & Meg. Alexandrou
Marousi 151 24, Athens, Greece

TP-04-15-827-EN-N

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu

ISBN: 978-92-9204-139-7
DOI: 10.2824/949547