Communication network interdependencies in smart grids - Annexes

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.

978-92-9204-140-3, 978-92-9204-140-3

Table of Contents

ANNEX A Communication protocols used in smart grids

SMART GRID DOMAIN	COMMUNICATION MEDIA AND LOW LEVEL PROTOCOLS
Last mile networks (FAN, NAN, AMI)	*Wired*: BPL (PLC), DLC (PLC), fibre, twisted pair, PDH, SONET/SDH, xDSL, POTS, PRIME (PLC), Meters&More (PLC), ANSI C12.18, ANSI C12.21. *Wireless*: radio frequency, microwave, cellular, GPRS, UMTS, LTE, IEEE 802.16 (WiMAX). *Medium independent*: TCP/IP suite, ANSI C12.22.
Backhaul Network	*Wired*: twisted pair, cable, fibre optic, POTS, SDH/SONET, PPP. *Wireless*: cellular, microwave, radio frequency, 3G, WIMAX, LTE. *Medium independent*: Frame Relay, ATM, MPLS, TCP/IP suite.
AMI networks	*Wired*: BPL (PLC), DLC (PLC), fibre, twisted pair, PDH, SONET/SDH, xDSL, POTS, PRIME (PLC), Meters&More (PLC), ANSI C12.18, ANSI C12.21. *Wireless*: radio frequency, microwave, cellular, GPRS, UMTS, LTE, IEEE 802.16 (WiMAX). *Medium independent*: TCP/IP suite, ANSI C12.22.
DER networks	*Wired*: serial, Ethernet, PPP. *Wireless*: radio, IEEE 802.15.4 ZigBee. *Medium independent*: TCP/IP suite.
Transmission grid networks	*Wired*: Serial Line, Ethernet, Frame Relay, PPP, ATM/TDM, BPL, DLC/PLC. *Wireless*: radio frequency, microwave, cellular, IEEE 802.16 (WiMAX). *Medium independent*: TCP/IP suite. IEC 61850 protocol family.
Link Layer/MPLS	*Wired*: Serial Line, xDSL, Ethernet, Frame Relay, PPP, ATM, TDM. *Wireless*: GPRS, Wi-Max, 2G, 3G, 4G, VSat, Wi-Fi, ZigBee. *PLC*: (Broadband Power Line, such as IEEE P1901 standard), DLC (Distribution Line Communications, such as PRIME), nb PLC (Narrowband PLC, such as Meters&More). *MPLS*: Multiprotocol Label Switching, it is “protocol agnostic” and commonly referred as layer 2.5.
Network Layer	*Medium independent*: IPv4, IPv6, IPsec.
Transport Layer	*Medium independent*: TCP, UDP, TLS/SSL.
Windmills	IEC 61850 protocol.
Hydro Power Plants	IEC 61850-7-410 protocol.
Other Systems	IEC 61850-7-420 protocol.

ANNEX B Advanced Metering Infrastructure (AMI)

In order to gather the necessary consumption readings for billing, DSOs make periodic roundtrips to each physical location to manually read the meters. The evolution towards smart grids, especially due to the use of Advanced Metering Infrastructures (AMI) and of smart meters in households, buildings and industry, will result in a situation where DSOs will be able to get these readings remotely and in an automated way.

The AMI infrastructure**Error! Bookmark not defined.** provides two-way communication between customers and utilities (i.e. DSOs), and it is one of the main ICT components used to smarten the power grid. This infrastructure depends heavily on the installation of smart meters.

There are other elements that are a basic part of the AMI, such as the underlying communication infrastructure, the central Meter Data Management systems or the intermediate meter data concentrators.

The AMI infrastructure needs an underlying communications' infrastructure network that provides communication between the different smart meters it controls, the intermediate data concentrators and the central Meter Data Management systems. Existing technologies, such as Power Line, Radio Frequency or Wireless networks are commonly used as a communication means between customer premises and AMI systems. These communications are bidirectional, as the control system can send command instructions to the smart meters when necessary. Again, security measures must be taken to protect these devices from cyberattacks and unauthorized access.

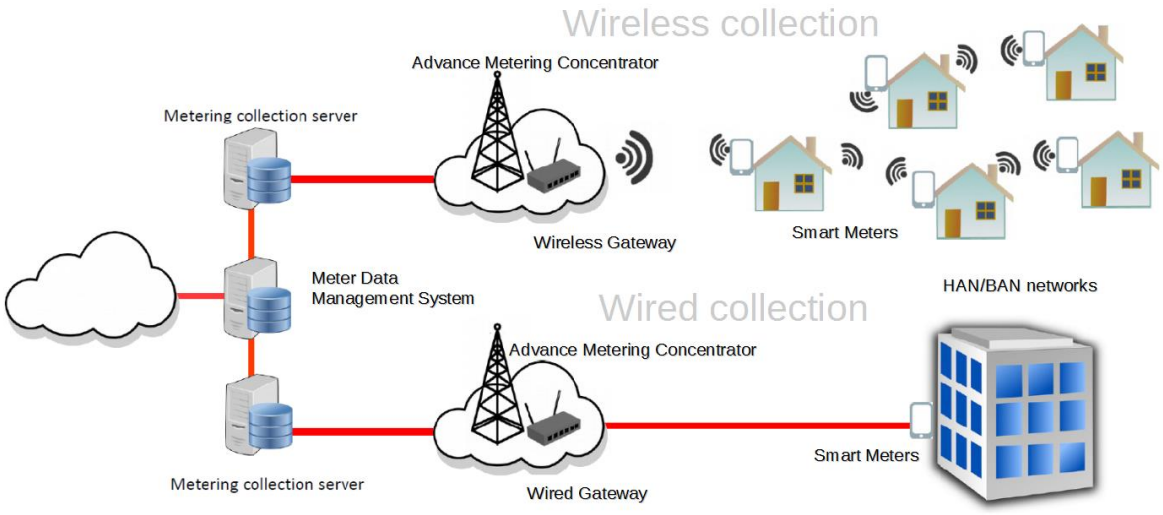
Meter data concentrators are control devices used between the Meter Data Management (MDM) and the smart meters. Meter data concentrators gather consumption and pricing data, and control the smart meters.

The MDM system is comprised of several components, the most important one being the protection, storage and management of customer data records. This includes sharing with third party actors and validating the data received from AMI systems.

B.1 Architectures and technologies used in AMI

Advanced Metering Infrastructures interconnect smart meter devices with utilities (DSOs). For this purpose, different protocols and architectures are used, depending on the needs of the network. However, commonly only two variations are used (as seen in Figure 1): PLC-based protocols (such as PRIME) in combination with DLMS/COSEM and wireless-based protocols, such as ZigBee in combination with technologies such as GSM.

Figure 1: AMI architecture.



As far as the PLC-based protocols are concerned, the PRIME protocol is one of the most relevant ones, alongside the DLMS/COSEM protocol for reading utility meters. Finally the ZigBee protocol will be discussed as a wireless communication example.

The **PRIME protocol** is a public, open, non-proprietary telecommunication standard that aims to satisfy the current and future needs of smart grids. It is based on international standards, and provides many interoperability features between devices from different manufacturers.

PRIME is divided into several layers:

- **Convergence Layer** (CL): classify network traffic according to the MAC layer that they belong to.
- **Media Access Control Layer** (MAC): provides access, bandwidth, connection management and topology resolution.
- **Physical Layer** (PHY): receive and transmit data packets between nodes, using OFDM modulation.

The device types according to the PRIME protocol are:

- **Base Node**: acts as a communication master. There can only be one base node per subnet, although there can be a backup one. It is the root of the PRIME tree.
- **Service Node**: they begin on a "disconnected" state, but when incorporated into a subnet they become "registered". They have two functionalities: to maintain the connectivity levels and to act as a switch to propagate the connectivity to other nodes.

Another alternative is the **Open Smart Grid Protocol** (OSGP), or GS OSG 001, which has been published by the European Telecommunications Standards Institute (ETSI). It is mostly used in the Netherlands and in certain Middle East countries. It defines a series of specifications focused on the control of smart grid applications over standard communication networks. It defines optimized, reliable and efficient delivery methods for command and control data to smart meters, including support for load control modules, gateways, solar panels, among others.

On a related note, the ETSI TS 103 908 standard for Power-line Telecommunications (PLT) is defined alongside the same lines as OSGP. The structure followed on this standard follows a similar approach to the OSI model, customized in order to meet the challenges that new smart grid technologies present.

Also the **Meters & More (M&M) protocol** is also used by several companies in Spain, Italy and Germany. It uses a centralized system that manages the network metering process. It focuses on increasing the robustness and agility of the communications' network. Provides the following features:

- Short message exchange method optimized for PLC systems.
- Use of 128bit AES encryption.
- Automatic network reconfiguration.
- Transmission management.

Moving on, one of the most widely used protocols for the implementation of advanced metering infrastructures is the **DLMS/COSEM protocol**. A version of this protocol, IEC 62056, is considered as an international standard, and is actively maintained by the IEC TC14 WG14 working groups. It is an application level protocol that works with the PLC-based protocols, mostly with PRIME.

This protocol defines a client-server architecture, where the smart meter is considered as a server and the end device as the client. This enables the smart meter to send commands and information directly to the client device, such as critical alarms, configuration information, etc.

More importantly, this protocol supports a series of features designed to provide an appropriate security level of its communications:

- **Message protection**: supports the use of cryptographic protection to the Application Protocol Data Units (APDU), ensuring the confidentiality and integrity of the information transmitted. AES-GCM-128 is used for the Data Transport Security of the APDUs, independently of the cryptographic protection that can be applied to the data before being sent.
- **Role-based authentication**: it is possible to establish peer authentication to data managed in a DLMS/COSEM server (smart meter). There are three levels defined:
  - ***Lowest level Security***: no authentication required.
  - ***Low Level Security*** (LLS): simple authentication required. Passwords are sent in clear text, and only the client devices need to be authenticated. This level of security is vulnerable to eavesdropping or replay attacks.
  - ***High Level Security*** (HLS): mutual authentication required. Both the client and server devices must authenticate mutually, using cryptographic primitives for this process. This level makes use of a 4-pass handshake process to verify the authentication of both devices before starting the information exchange.

Another widely used protocol is **ZigBee**, which is almost exclusively used for low-power applications. In fact, this protocol has been designed especially for this kind of application, establishing as base those capable of low data rates (250 kbps or less). It is mostly used through a PHY/MAC layer of the IEEE 802.15 standard, although it is technically possible to use it through a Power Line Communication.

This protocol offers a series of security measures to protect communications. To verify the communications, ZigBee makes use of certificates, provided by ZigBee Alliance members that uniquely identify each device.

The communications are secured using AES encryption, and the keys required are computed by using these certificates.

Another option is the use of the IEEE 802.15.4 protocols, which is focused more on the physical layer and media access control, specifically on lower-rate wireless networks. It is commonly used in conjunction with ZigBee, serving as a base as it covers a different set of layers.

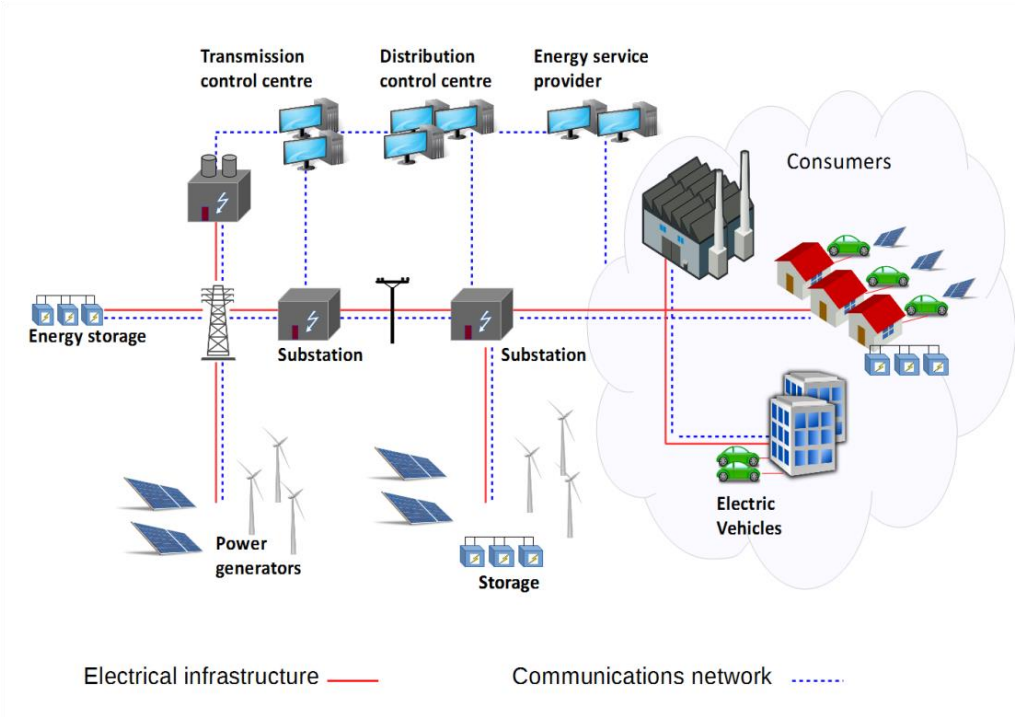
However, it is important to take into account that DLMS/COSEM, ZigBee and IEEE 802.15.4 do not provide any key management functionalities, and these have to be added later on an application level.

Finally, there are also other protocols and technologies that can be used in AMI networks, as can be seen on the table on ANNEX A.

ANNEX C Distributed Energy Resources (DER)

Distributed Energy Resource (DER) systems include generation and storage systems, both renewable (photovoltaic systems, wind turbines, bio-fuel systems, fuel cells, battery storage systems, electric and thermal storage systems, co-generation systems and small hydro plants) and non-renewable (diesel generators, gas turbine generators, etc.)[1]. Figure shows a model of a possible architecture for a DER system within a smart grid network, distinguishing the electrical infrastructure and the communications infrastructure.

Figure 2: Distributed Energy Resource (DER) smart grid diagram.



Each type of DER system has its own unique characteristics but, in general, they can be treated as a small to medium-sized sources of electric power. Electric Vehicles (EVs) can sometimes act as DER systems, however as they have different purposes, they are usually identified as a separate entity from the rest of DER systems.

DER systems are located at residential, commercial, and industrial customer sites and are usually owned and managed by the utility customers located at those sites. Utility-owned DER systems can be located at utility sites, such as substations, or may be located by mutual agreement at customer sites (e.g. rent-a-roof contracts).

Due to the distributed nature of these DER systems, it becomes necessary to properly interconnect them with the rest of the smart grid network. These communication networks must cover all the devices from these systems, in order to enable remote control from the utility and operation centres and ensure their efficient interaction within the whole grid. Furthermore, as they are distributed, and on more than one

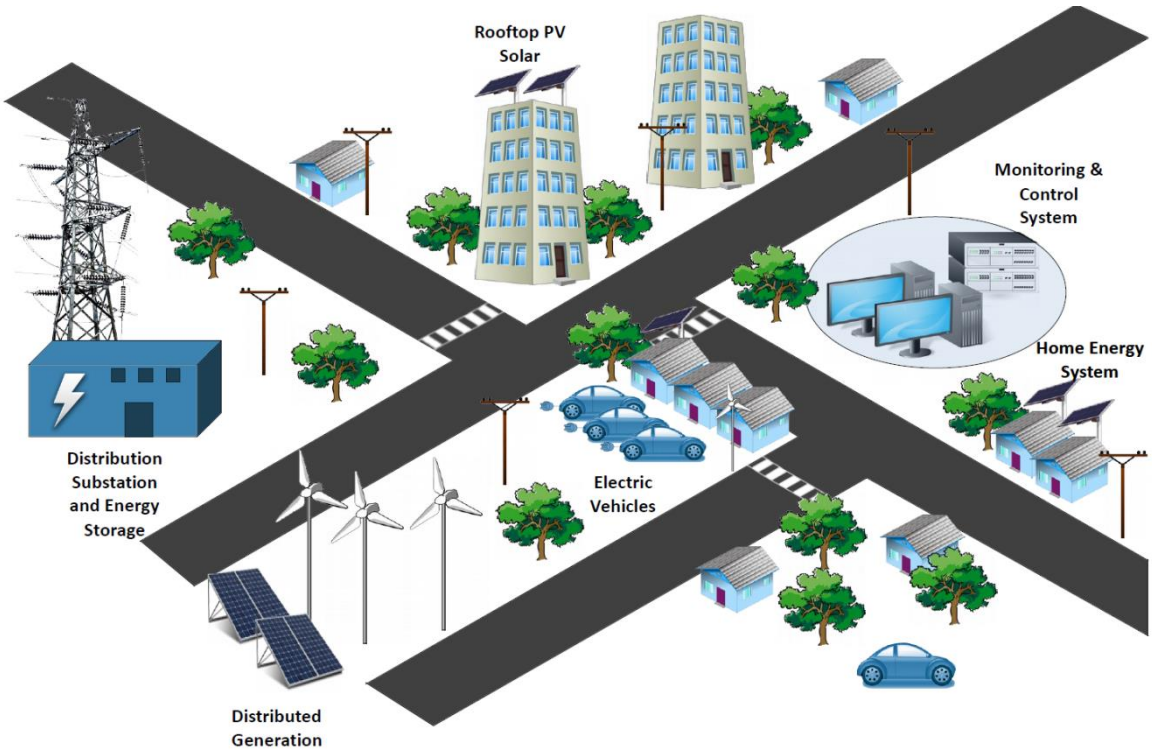
[1] NESCOR. "Cyber Security for DER Systems", July 2013.

occasion will make use of the Internet network, these communications will need to be secured to protect them from attacks and accesses from unauthorized users.

C.1 Utility responsibilities for DER Systems interconnected to their smart grids

Utilities do not typically have direct organizational control over these DER systems and often need to operate through the DER owners, commercial Retail Energy Providers, Aggregators, Virtual Power Plant managers and other third parties. Figure shows a sample illustration of some of the possible DER systems that can provide energy to the new smart grids, ranging from utility-scale providers to basic home energy systems (such as solar panels or windmills).

Figure 3: Distributed Energy Resources.



In addition, many DER systems will be located at customer sites that have little or no security at all, and with owners who have minimal or no cyber security expertise. Unlike utility-owned smart meters, the customers must be allowed to interact with the DER systems that they own, since they often use these systems to meet their own specific needs. These factors can increase the risks posed by the cyber-security vulnerabilities of the interfaces between DER systems and Utilities. Apart from these interfaces, the communications infrastructure and networks used by these devices to communicate must also be protected against these vulnerabilities and risks.

C.2 Utility Management of DER Systems

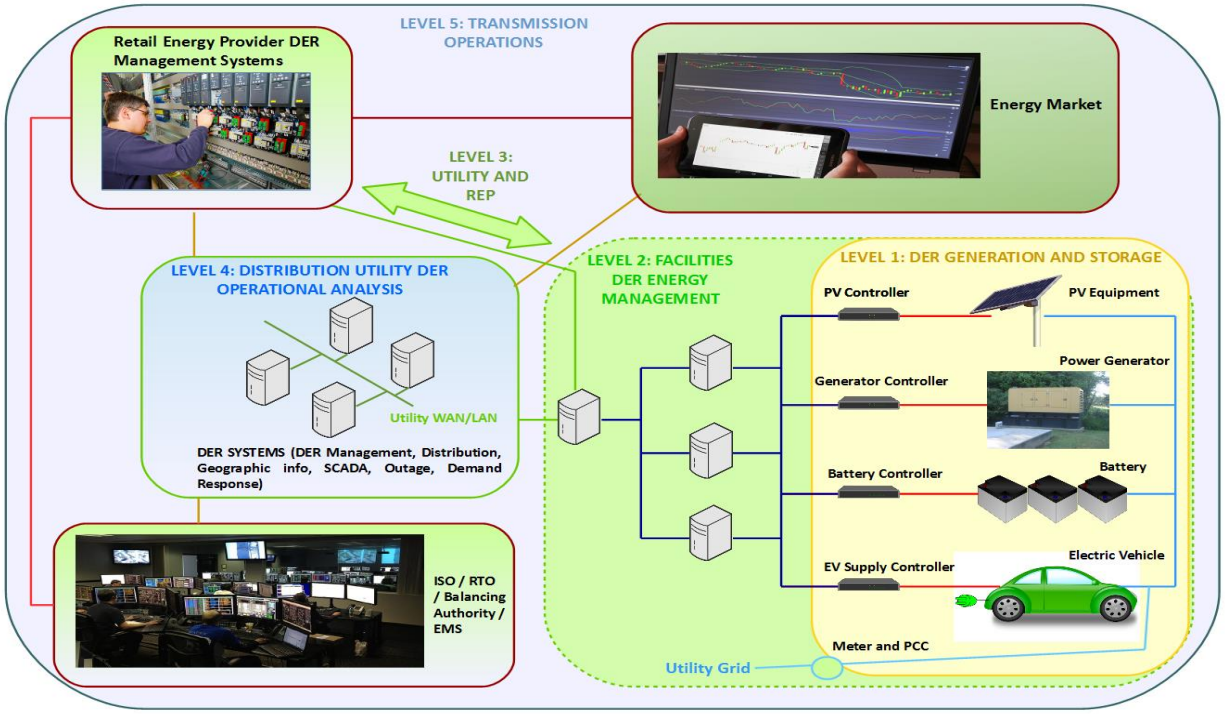
New methods for handling these dispersed sources of generation and storage are being developed, including both new power system functions and new communication capabilities. In particular, the smart capabilities

of DER systems will be utilized to allow power system management to take place locally and within the utility environment. This last point brings us to the previously commented risk, by distributing the control and management of the network, it is imperative that the communications' infrastructure and networks get secured against external unauthorized access and other threats.

C.3 Architectures and technologies used in DER

Hierarchical architectures are commonly used for the implementation of DER systems in smart grids. On Figure a typical implementation of this hierarchy can be observed. The architecture is divided into five levels, from the lowest level (DER Generation and Storage) to the highest level (Transmission and Market Operations).

Figure 4: Hierarchical DER System Architecture.



The levels defined for the Hierarchical DER System Architecture are described in more detail on the following points:

- **Level 1**: Autonomous DER Generation and Storage is the lowest level and includes the cyber-physical DER systems. These DER systems will be interconnected to the utility grid and will usually operate autonomously according to pre-established settings.
- **Level 2**: Facilities DER Energy Management is the next higher level in which a facility DER management system (FDEMS) manages the operation of the Level 1 DER systems. This FDEMS can manage DER systems in residential, commercial and industrial sites.
- **Level 3**: Utility and REP (Retail Energy Providers) Operational Communications extends beyond the local site to allow utilities and possibly REPs to request or require DER systems (typically through a FDEMS) to take specific actions. The settings for autonomous DER operations are modifiable by utilities and Retail

Energy Providers. Controls include turning on or off devices, setting or limiting output, providing ancillary services (e.g. Volt-Var Control), and other grid management functions.

- **Level 4**: Distribution Utility Operational Analysis applies to utility applications that are needed to determine which requests or commands should be issued to specific DER systems. Utilities monitor the power system and assess if efficiency, reliability, or market advantage can be improved by having DER systems modify their operation. This utility assessment involves many utility control centre systems, including GIS, DMS, OMS and DR systems, as well as DER Management Systems (DERMS).
- **Level 5**: The transmission and Market Operations is the highest level, and it involves the broader utility environment. RTOs (Regional Transmission Organizations) or ISOs (Independent System Operator) may need to exchange information about the capabilities and operational status of larger DER systems and/or aggregated DER systems.

Regarding applicable protocols for these systems, the IEC 61850 provides integration with DER Grids through the IEC 61850-90-15 integration standard. It defines a hierarchical DER system, controlled by a DER management system connected to other DER systems, interfacing with endpoint DER units. It also defines the information model to use when connecting with other systems that use protocols defined within the IEC 61850 standard. This standard focuses on three main core components:

- Information exchange and communication protocols.
- Application modelling and logical nodes.
- Engineering and configuration language.

From these components, the protocols aim to achieve the following goals:

- Reduce implementation costs.
- Achieve interoperability among different products and technologies.
- Enable seamless integration among these devices.

For power system and supply security reasons, DER systems have to include ancillary services that are commonly seen on traditional power systems or bulk generation systems, as to ensure compatibility with older and legacy devices and systems.

Therefore, secure communications are essential in order to interconnect all these layers and ensure that the operations and control instructions are properly transferred from one end to the other. Lack of security in this aspect could allow unauthorized users or attackers to modify control transmissions, intercept sensitive or personal information (such as consumption habits), and even be used in order to damage the network by causing system instability, energy outages, blackouts, etc.

These layers will be intercommunicated using a combination of different technologies that will vary depending on the needs of each individual implementation (the most commonly used protocols and technologies are listed in ANNEX A).

ANNEX D Detailed threats to smart grid interdependencies

This annex details the treats that were listed on the table on **Error! Reference source not found.**, sorted by the domains that have been defined:

D.1 Nefarious activity

- **Advanced Persistent Threats** (APTs): these attacks are usually carried out by large organizations or groups, as they require capacity to continuously monitor their objective in order to be able to attack and extract information from a specific target. This kind of attack always has direct human involvement to be orchestrated (contrary to what happens with many virus, Trojans, worms and malicious code that can spread without direct human interaction).
- **Channel jamming**: is one of the most efficient ways to launch physical-layer Denial of Service (DoS) attacks, especially when targeting wireless networks.
    - ***Distributed Denial of Service*** (DDoS): attacks focused on disrupting services, data exchanges, or communications by introducing noise to the network, or saturating a service with large quantities of requests. These attacks are commonly launched to interrupt communications with concentrators in smart grids.
- **DNS attacks**: are commonly focused on impeding or altering the name resolution system in order to interrupt operations or redirect users to malicious devices. While this resolution is mainly used for human use (is easier to remember a web address than an IP), some services can make use of it too.
    - ***DNS registrar hijacking***: the DNS server is compromised, and therefore any resolution that it contains can be altered or made unavailable.
    - ***DNS spoofing/poisoning***: are a group of threats focused on attacking the DNS servers in order to introduce forged information to redirect a user or system to a malicious service or simply to redirect them to an invalid site to interrupt communications.
- **Generation and use of rogue certificates**: these certificates can be used to perform MITM attacks, masquerade an attacker as a legitimate system, etc.
- **Identity theft**: steal valid credentials in order to gain illicit access to the systems and obtain sensitive or private information.
- **Injection attacks**: these attacks are based on the injection (of packets, code, SQL…) in order to obtain access to systems, damage networks or devices, compromise information integrity, etc.
    - ***Malicious code injection***: inject malicious code into the systems in order to obtain access, disrupt its service or damage it. Commonly these injections are used in combination with exploits.
    - ***Malformed data injection***: send manipulated or malformed data packets to the devices and systems on the network in order to disrupt or damage them.
- **Malicious code**: malicious components capable of infecting devices and systems, which can cause different effects depending on the objective of the attacker (enable backdoors for attackers, modify security parameters, steal information, corrupt the system, etc.).

  - ***Exploit kits***: exploits are very well known attack vectors through which malicious code can be injected into a target system to gain access or cause system instability. They make use of unpatched vulnerabilities on the systems.
  - ***Virus/worms/Trojans/Malware***: different varieties of malicious code that can have different effects and that can be distributed through a variety of channels (such as email, attachments or exploits).
- **Social Engineering**: an attacker coaxes an employee into unknowingly revealing sensitive information, credentials or access codes.
  - ***Phishing***: a type of social engineering attack where the attacker masquerades as a trustworthy entity in order to obtain sensitive information, credentials or personal information.
- **Unauthorized access to systems**: attacks focused on gaining access at different levels on restricted systems.
  - ***Password attacks***: the most common overlook is the use of default passwords. This is risky, as there can be millions of devices with the same default password, and therefore they are at risk of being accessed without authorization. Another point of concern is the need to have a robust password policy to ensure that the passwords used are not easily guessable.
  - ***Privilege escalation***: when unauthorized users gain administration privileges within a system.
  - ***Unauthorized software installation***: by installing unauthorized software into a system, that system becomes at risk, as it was not meant to be run in the first place and can cause incompatibilities, resource saturation, etc.
  - ***Use of restricted software***: restricted software should be protected to avoid its accidental use or misuse by unauthorized users.
- **Web-based attacks**: these attacks focus on the vulnerabilities that the web interfaces that some of the systems can have, in order find attack vectors to carry out more specific attacks.
  - ***Administration interfaces***: these interfaces must be properly secured as they allow access to advanced functionality. These interfaces should ideally not be accessible from the Internet.
  - ***Web services/applications***: these applications can be attacked in order to gain access to systems or to steal information.

D.2 Eavesdropping, interception and hijacking

- **Information theft**: this refers to an unauthorized real-time interception of private communications. This also affects private consumer information, including data such as energy consumption, contract details or which devices are connected to the network.
- **Man-in-the-Middle**: active eavesdropping attack, in which the attacker makes independent connection to the victims and relays messages from one to another, in order to make them believe that they are talking directly with each other.
  - ***Man-in-the-Middle Masquerade***: these attacks can be used to intercept communications between systems, especially on wireless networks, acting the attacker as a middleman: appearing as the server for the client and the client to the server; therefore obtaining secure connections with both but having access to the unencrypted traffic.
  - ***Mobile network interception***: there are systems already available capable of intercepting mobile communications by disguising themselves as legitimate network provider hotspots. A recent example is the commercially available Typhoon HX offered by the NSA.

  - ***Session hijacking***: stealing the meter connection by acting as a legitimate host, or by acting as a fake DR system, in order to steal, modify or delete transmitted data.
  - ***Wireless network interception***: with the appearance of drones, new means of intercepting communications have appeared. The most common one is comprised of fitting a drone with surveillance equipment capable of intercepting and carrying out MITM attacks from the sky on poorly secured wireless networks. An example is the SPARROW II micro-computer.
- **Network reconnaissance, information gathering**: passively obtain internal information about the network: architecture, infrastructure, devices connected, protocols used, etc.
- **Replay of messages**: this attack uses a valid data transmission maliciously by repeatedly sending it or delaying it, in order to manipulate or crash the targeted device.
- **Routing attacks**: these attacks focus on damaging the interconnections within the network in order to interrupt, misconfigure or intercept communications.
  - ***Address space hijacking***: attacks on the routing systems in order to redirect traffic towards a public or compromised network where the attacker will be able to eavesdrop or intercept sensitive or private communications.
  - ***Autonomous System (AS) hijacking***: these attacks impersonate the identity of the victim's organization to carry out malicious activities or manipulated instructions pretending to be the victim itself. To avoid this, it is necessary to use origin validation through the use of certificates.
  - ***Route leaks***: improperly configured routes can cause communications to be sent through unsecure or untrusted networks, where the information will be vulnerable to interception.
- **Smart Meter connection hijacking**: unauthorized communication with the DR system in order to illicitly obtain or modify information.
- **War driving**: act of locating and trying to exploit connections to wireless local area networks while driving around the installations of the target organization.
  - ***War flying***: a new variety of this threat has emerged recently, where instead of driving around with surveillance equipment, a drone is used instead. These drones have better access (can for example be placed on the ceiling of a building, and can intercept wireless networks and attack them. There are commercial versions available, but the mayor threat comes from the custom ones that can be made by enthusiasts and amateurs quite cheaply.

D.3 Deliberate data damage

- **Information integrity loss**: a malicious attacker could access the systems in order to damage or delete sensitive information stored, or communications in transit, in order to disrupt the proper operation of the smart grid devices.
- **Information leakage**: a malicious attacker or user deliberately leaking internal sensitive or private information to the general public. This information can have different impacts, such as serving as a staging area to plan more advanced attacks, blackmail employees or the company itself, or even result in band damage.
- **Information manipulation**: in this case, the objective is not to damage the systems, but to manipulate the information in order to cause chaos, or monetary gain. An example of this would be modifying the accounting and billing information in order to reduce (or increase) consumption values, which impact directly on the users.

- **Trusted firmware**: the firmware used on the devices and systems has to be signed and verified, to ensure that it is valid and trusted. Running untrusted firmware can lead to the execution of untrusted code, unauthorized access and manipulation / corruption of the data it manages.

D.4 Unintentional data damage

- **Configuration errors**: poorly or erroneously configured systems are prone to be put at risk, as bad configurations can potentially allow attacks to be successful.
- **Channel interference**: it usually affects the availability of the PLC channel, and it's usually caused by network noise caused by damaged wiring, faulty systems or environmental noise.
- **Erroneous information sharing, leakage**: Lack of discretion of the personnel could lead to unauthorized interception of private communication, including accidental leaks; such as sending sensitive information to the wrong e-mail.
- **Erroneous use of devices, systems and administration interfaces**: incorrect use of administration interfaces and devices is a serious risk, as these interfaces offer advanced management features that if improperly used, can damage devices, cause outages, etc.
- **Unintentional data alteration**: a user accidentally modifying information can have serious repercussions if this information, for example, regulates a critical system, or distribution station.
- **Usage of information from an unreliable source**: using data without verifying the source can be a severe security risk. If an RTU does not verify the origin of the orders it receives, a malicious user could intentionally send erroneous orders that could corrupt the device or disrupt the energy supply.

D.5 Outages

- **Communication system (network) outage**: lack of communications stops the systems from being able to communicate between themselves and the control systems.
  - ***Network outage cascade effect***: if the systems are not properly configured, a failure in one node could spread and indirectly affect other nodes, causing them to fail too as was described on Chapter **Error! Reference source not found.**, **Error! Reference source not found.**.
- **Energy supply outage**: it stops devices from working, or communicating if the failure occurs on intermediary devices, causing blackouts or energy loss on the affected segments.
  - ***Energy supply outage cascade effect***: if the grids are not properly interconnected and configured, an outage in one section of the network could affect negatively other segments, causing more outages or overloads in sections not directly related to the one that failed.

D.6 Other threats

There are a series of threats that can affect smart grid communication networks, but that are not related directly with the cybersecurity and as such are not the main focus of this report. However, it is important to always have them in mind in order to obtain the whole picture:

- **Deliberate physical attacks**: incidents such as infrastructure element theft, bomb attacks, vandalism or sabotage could damage communication lines or devices, or stop relevant personnel from properly carrying out their tasks.
- **Failures & malfunctions**: device and communication lines failures or malfunctions can stop services from communicating and working properly.
- **Natural disasters**: these include events such as fires, floods, environmental disasters or earthquakes, which could physically damage the communication lines.
- **Future technologies**: an often overlooked point includes the evaluation of the technologies to come and the risk they can pose to current and forthcoming installed systems; these technologies, which are continuously in evolution and could, theoretically, invalidate current cryptologic techniques. If these considerations are not taken into account, replacing security measures in place on smart grids in the future could prove time and cost-prohibitive.
    - ***Quantum computing***: these new technologies threaten current Public key Crypto-Algorithms which are based mostly on RSA or Elliptic Curve, and many manufacturers are already working on them and developing proofs of concept regarding their potential.
- **Unintentional events**: despite the fact that they are cannot be considered as attacks, unintentional events can become threats and put the overall systems at risk.
    - ***Unintentional data corruption***: users manipulating information uncontrollably can put that information at risk of being modified or deleted unknowingly.
    - ***Unintentional data leakage***: if users are not aware of the security procedures that have to be followed when handling data, it can lead to the data being unintentionally leaked (send though an unsecured channel, copied into removable media without encryption, etc.).
    - ***Unintentional misconfigurations***: configuring or maintaining a device without fully understanding the security measures that must be in place, could lead to a device to be exposed as a configuration parameter invalidates already existing security measures.

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-04-15-828-EN-N

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

ISBN: 978-92-9204-140-3
DOI: 978-92-9204-140-3