SecureGrid

Deliverable

SotA (State-of-the-Art) Documentation

Editor: ERICSSON

ITEA 3 Project 14039

December, 31st of 2020

SecureGrid 20 YEARS ITEA 3 1998 - 2018

Document properties

Distribution	Public
Version	2.0
Editor	Ericsson
Authors/ Contributors	Ericsson / Cem Pancar SOTEC / David González García Gerade Software / Gökhan Yanmaz Baskent / Ozden Ercin Experis / Ester Peña Nimbeo / Angel Lagares
Pages	28

Abstract

This document describes describe the current technological situation in the project domain with a detailed technical State-of-the-art (SotA), with regard to current products, prototypes and research results and trends, both on the industrial and academic sides. This document is an extension of the SotA delivered in the FPP reason why is being delivered as public deliverable.

Table of contents

1 Introduction

The European Technology Platform[1] defines “a Smart Grid as an electricity network that can intelligently integrate the actions of all users connected to it – generators, consumers and those that do both, in order to efficiently deliver sustainable, economic and secure electricity supply”.

According to National Institute of Standards and Technology (NIST) [2] a smart grid is "a modernized grid that enables bidirectional flows of energy and uses two-way communication and control capabilities that will lead to an array of new functionalities and applications."

A huge change from the traditional grids is among the type of flows in the grid that now include not only electricity delivery but a two-way flow of both electricity and data. Data gathered in real time assure the information needs to improve efficiency, reliability, and allow the electrical operator to manage the grid in a more “intelligent” way. While integrating information technologies is essential to building the smart grid, the same networked technologies add complexity and also introduce new interdependencies and vulnerabilities.

[1] www.smartgrids.eu

[2] www.nist.gov

2 Smart Meters and Automatic Metering

Smart meters are electronic devices that record/measure customer consumption, and other parameters, in time intervals of an hour, or less, and send that information over a communications network, to the utility for monitoring and billing[3].

It is important to highlight the difference between automatic meter reading (AMR) and advanced metering infrastructure (AMI). All AMI systems contain AMR functionality, but all AMR systems are not AMI systems. Because of the inherent differences in AMR and AMI, the data available from each system differentiates them. Basically, advanced metering infrastructure (AMI) differs from traditional automatic meter reading (AMR) in that it enables two-way communications with the meter and typically provides substantial information, including: Cumulative electric energy usage; Daily electric energy usage; Power peak demand; Last interval demand; Load profile; Voltage value; Voltage profile; Phase information; Outage counts; Tamper notification; Electric energy time-of-use (TOU) and power peak readings.

With AMI systems nearly, all this information is available in real time and on demand, allowing for improved operations and customer management. AMI systems can also be used to verify power outages and service restoration, perform remote-service disconnects and reconnects, allow automated net metering, transmit demand-response and load-management messages, interrogate and control distribution-automation equipment and facilitate prepaid metering.

AMI provides the data that can be handled by means of AI and Big Data techniques to smooth these uncertainties In addition, demand response and pricing programs that can be implemented via AMI systems allow the utility and customers a number of options to manage their usage.

3 Sensor Networks

Sensor Networks (SNs): are considered to be one of the most suitable technologies for smart grid (SG) technology – due to their low-cost, collaborative and long-standing nature. Wireless sensor networks (WSNs) can enable both utilities and customers to transfer, monitor, predict, measure, and manage energy usage effectively, as shown below. Thus, WSN can revolutionize the current electric power infrastructure by integrating information and communication technologies (ICT) [4], [5].

[3] Federal Energy Regulatory Commission, “Assessment of Demand Response and Advanced Metering”, FERC-Department of Energy, Staff Report, December 2008

[4] W. Wang, Z. Lu, “Cyber Security in the Smart Grid: Survey and Challenges,” Computer Networks, 57 (2013), 1344-1371.

[5] Grilo et al., “A Wireless Sensors Suite for Smart Grid Applications,” The International workshop on information technology for energy, 2012.

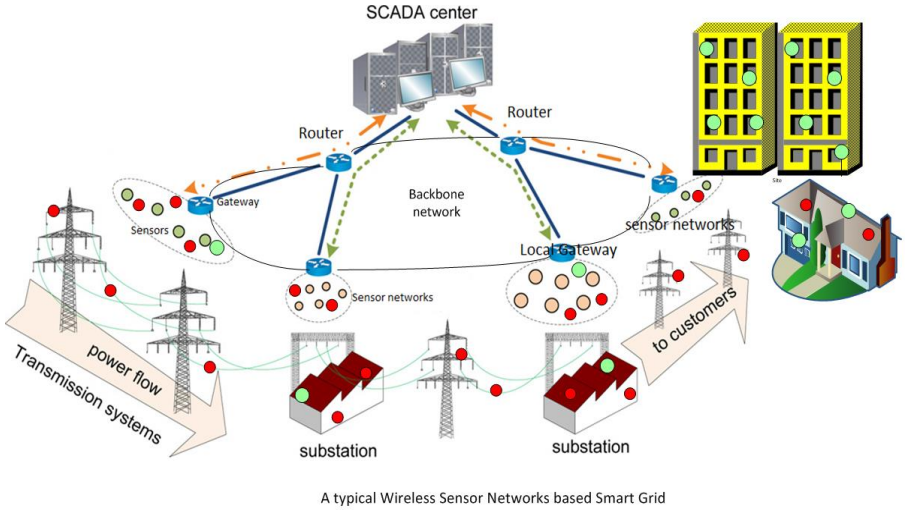


Figure 1. WSN-based SG.

Such a heavy dependence on ICT networking inevitably surrenders the SG to potential vulnerabilities. Thus, security emerges to be a critical issue because millions of heterogeneous devices (e.g., sensors, etc.) are inter-connected via communication networks. In smart grids, as security challenges mainly come from malicious cyber-attacks via communication networks, it is essential to understand potential vulnerabilities under network attacks, e.g., denial of service (DoS), eavesdropping, and masquerading attacks, list of few [6]. Hence, robust authentication schemes are required to detect and response the malicious attacks (e.g., DoS).

As SG network consists of thousands of nodes that are resource-hungry (less memory, battery power, and less bandwidth) with limited computational ability, therefore, computational efficient security protocols (e.g., authentication and key management architectures) becomes an important factor that could detect and tolerate the faults and attacks in the Smart Grid [7,8]. E.g., in power substation, if a sensor that keeps monitoring the status of a power feeder senses any anomaly (e.g., high voltage/current), it will issue a command of tripping circuit breakers to protect power equipment. The most efficient way is to multicast a time-critical message to all related breakers that belong to the same multicast group. Hence, authentication schemes in the SG must be able to efficiently support multicast[9]. [10] proposed a key-management architecture for secure SCADA communications

[6] Y. Liu, "Wireless Sensor Network Applications in Smart Grid: Recent Trends and Challenges," International Journal of Distributed Sensor Networks, vol. 2012, Article ID 492819, 8 pages.

[7] S. Iyer, "Cyber Security for Smart Grid, Cryptography and Privacy," International Journal of Distributed Sensor Networks, vol.2011, Article ID 372020, 8 pages.

[8] H. Khurana, R. Bobba, T. Yardley, P. Agarwal, E. Heine, "Design principles for power grid cyber-infrastructure authentication protocols," in: Proc. of the Forty-Third Annual Hawaii International Conference on System Sciences (HICSS '10), 2010

[9] N. Liu, J. Zhang, W. Liu, "Toward key management for communications of wide area primary and backup protection," IEEE Transactions on Power Delivery 25 (2010) 2030–2032.

but it is less efficient during the multicast process. [11] proposed SMOCK to achieve light-weight key management for power grids. SMOCK is not fully designed with multicast. Hence, it goes without saying that a trade-off between robust security and latency is still needs to be explored in the SG.

4 Big Data and Artificial Intelligence

The European Union (EU) wants more than two thirds of Europe's electricity users to have smart meters by 2020. The diversity and huge amounts of data that smart meters and automatic meter infrastructures make available is crucial to achieve the goals of an efficient and intelligent grid, but can only be useful if tools to gather, analyse and obtain knowledge from it are employed.

Big Data is intended to put together all data coming from Automated Metering Infrastructure, while Artificial Intelligence Techniques can be used to extract knowledge and derive decision support at various levels and to different players.

For several studies, the quality of the databases is essential, as well as other additional information that can influence the electricity usage such as the type of activity, hired power value, electric energy consumption, the weather, etc.[12] Indeed this is a domain where data increases exponential while the number of smart meters is spread to all clients; the data comes at different time intervals, from different sources, it is of several different types, and usually is complex data and unstructured one, so, only Big Data techniques can deal with this torrents of data in near-real time.

Some initiatives are already being approached in on-going projects such as some ITEA projects (SEAS[13] and IMPONET[14]) and are encouraging, and the fact is that worldwide industry is currently investing on the development of advanced devices and appliances that allow the online monitoring and control of consumption. Some platforms already exist that gather data consumption allow consumers to obtain and compare their profiles with consume. The Green Button Initiative[15] started in September 2011 as a result of collaboration among the White House, NIST, state regulators, utilities, vendors and North American Energy Standards Board. Green Button enables electronic consumer access to energy data (contains no Personal Identifiable Information) and supports development of ecosystem (apps), having 48 utilities and more than 42M of customers.

---

[10] D. Choi, H. Kim, D. Won, S. Kim, “Advanced key-management architecture for secure SCADA communications,” IEEE Transactions on Power Delivery 24 (2009) 1154–1163.

[11] . He, Y. Huang, R. Sathyam, K. Nahrstedt, W.C. Lee, “SMOCK: a scalable method of cryptographic key management for missioncritical wireless ad-hoc networks,” IEEE Transactions on Information Forensics and Security 4 (2009) 140–150.

[12] S. Ramos, J. Duarte, J. Soares, Z. Vale, F. J. Duarte, "Typical Load Profiles in the Smart Grid Context – A Clustering Methods Comparison". IEEE Power and Energy Society General Meeting, USA, 2012.

[13] http://www.the-smart-energy.com

[14] http://www.innovationenergy.org/imponet

[15] http://energy.gov/data/green-button

However, the amount and type of data that it is possible to obtain from the grid will be useful only if, besides being gathered and structured by means of efficient Big Data techniques, knowledge can be extracted from it.

Artificial Intelligence (AI) techniques are currently being employed, and Neural Networks (NNs) is one of the most used AI techniques, particularly suitable for problems characterized by a high complexity and great variation in the problems' data[16], such as electricity market prices forecast[17], load harmonics prediction[18], consumption forecasting[19] among many other.

In the last years, significant research efforts have been devoted to clustering techniques in order to obtain daily load profiling[20],[21]. In[22] typical load profiles are accomplished based on the Fuzzy C-Means (FCM) algorithm for consumers with hired power above 41 kW. In[23] an original application of Support Vector Clustering (SVC) is presented for classification of electrical consumers patterns.

Another domain where research is still in progress is the use of AI techniques for consumers' characterization. Some examples include Data Mining techniques used to establish load profiles taking into account the effect of weather conditions[24]. In[25] an electricity consumer's

[16] Babu, G.S.; Suresh, S., "Sequential Projection-Based Metacognitive Learning in a Radial Basis Function Network for Classification Problems," IEEE Trans. Neural Networks and Learning Systems, vol.24, no.2, pp.194,206, Feb. 2013.

[17] N. Amjady, A. Daraeepour, and F. Keynia, "Day-ahead electricity price forecasting by modified relief algorithm and hybrid neural network," IET Gener. Transm. Distrib., 2010.

[18] J. Mazumdar, R. G. Harley, F. C. Lambert, and G. K. Venayagamoorthy, "Neural Network Based Method for Predicting Nonlinear Load Harmonics," IEEE Trans. Power Electron., vol. 22, no. 3, pp. 1036–1045, May 2007

[19] L. Hernández, C. Baladrón, J. M. Aguiar, B. Carro, A. Sánchez-Esguevillas, J. Lloret, "Artificial neural networks for short-term load forecasting in microgrids environment", Energy, Vol. 75, October 2014, Pages 252-264, ISSN 0360-5442, http://dx.doi.org/10.1016/j.energy.2014.07.065

[20] A. Mutanen, M. Ruska, S. Repo, P. Jarventausta, "Customer Classification and Load Profiling Method for Distribution Systems". IEEE Transactions on Power Delivery, vol.26, no.3, pp.1755-1763, 2011

[21] M. Halkidi, Y. Batistakis, M. Vazirgiannis, "Clustering algorithms and validity measures". Tutorial paper in the proceedings of the SSDBM 2001 Conference

[22] D. Gerbec, S. Gasperic, I. Smon, F.Gubina, "Allocation of the load profiles to consumers using probabilistic neural networks". IEEE Transactions on Power Systems, vol.20, no.2, pp. 548- 555, May 2005

[23] G. Chicco, S. Ilie, "Support Vector Clustering of Electrical Load Pattern Data". IEEE Transactions on Power Systems, vol.24, no.3, pp.1619-1628, August 2009

[24] Young-Il Kim, Shin-Jae Kang, Jong-Min Ko, Seung-Hwan Choi, "A study for clustering method to generate Typical Load Profiles for Smart Grid". Power Electronics and ECCE Asia (ICPE & ECCE), on IEEE 8th International Conference, May 30-June 3 2011

characterization study is conducted, which involved the analysis of load curves of 155 customers belonging to the medium voltage distribution systems in the north of China. This approach used three clustering algorithms: k-means, fuzzy c-means and self-organizing maps (SOM) in order to grouping the typical daily load diagrams. An important issue is the attention on Data Privacy related to the deployment of Smart Grids. It implies the implementation of information protection and access control.

5 Information and Communication Technologies

Due to the increased usability of smart grid environment, utility operators are forced to use known and new trend communication solution to collect data, manage the edge devices such as meters, remote terminal units or sensors and also control any behavior change of difference from ground zero stage.

Based on the grid structure and expectations different type of communication solutions have been selected over the years to embed into power grid structure. Unfortunately, there is not a single solution or technology fitting all expectations of today and of the future. With regard to availability of wires or wireless environment, utility operators did select public networks as well as private structure to collect necessary data from the remote fields.

Several examples can be seen in energy grid levels as well as based on different regions. Transmission lines more served by fiber optical line (OPGW – Optical Ground Wire, ADSS – All Dielectric Self Supporting) or High Voltage PLC (Power Line Carrier), whereas distribution lines uses more cellular networks, low / medium voltage PLC, RF (radio frequency) or new trend of unlicensed wireless solutions (Sigfox, LoRa, Weightless, Ingenu etc.).

Based on European Region, cellular communication as well as PLC is heavily use. North America is more a region where the utilities using RF technologies based on the coverage of area, investment of available communication solutions and usage difference.

to it. Information and Communication Technologies (ICT) are crucial for the success and implementation of the Smart Grid concept. There are several communication technologies that could support Smart Grid communication in the distribution system, ranging from optical fiber, to power line carrier (PLC), to wireless technologies[26].

A three-level hierarchy can be defined for smart grid communication network which includes the Home Area Network (HAN), Neighborhood area network and Wide Area Network (WAN). An overview of the AMI communication scheme is shown below.

[25] S. Ramos, João Duarte, João Soares, Zita Vale, Fernando J. Duarte, "Typical Load Profiles in the Smart Grid Context – A Clustering Methods Comparison". IEEE Power and Energy Society General Meeting 2012, San Diego CA, USA, July 22 - 26 2012

[26] [9] Stephen F. Bush, “Smart Grid: Communication-Enabled intelligence for the Electric Power Grid”, IEEE Press, John Wiley & Sons Ltd. Ed., 2014

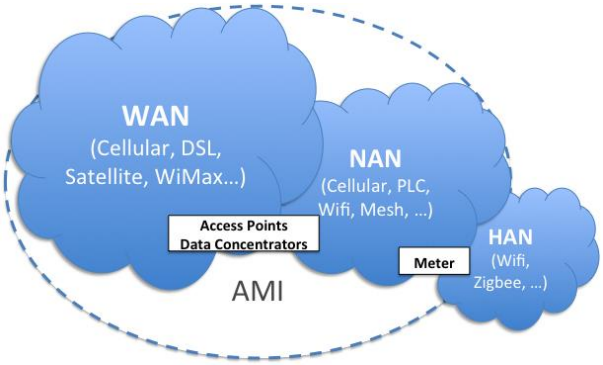


Figure 2. Overview of AMI networks.

With ICT-enhanced infrastructures, grids are evolving from centralized and hierarchical topologies to distributed and holonic architectures. They provide substantial added value in terms of efficiency, eco-friendliness and savings. However, a major brake to their adoption is the security issues they raise. With enhanced communication, load balancing automation and big heterogeneous data analysis capabilities, the grid becomes vulnerable to large scale cyber-attacks, aiming to steal consumer data, cheat on metering or even tear down the infrastructure. Hence, security is to be seen as a "market enabler" to smarts grids.

Warwick Ashford[27] reports that United Kingdom (UK) consumers believe that e smart meters will capture too much personal information and will be vulnerable to cyber-attack. Almost 80% believe smart meter PII will require additional security and 73% believe consumers should own smart meter PII data.

An identified method of attacking the meters involves placing a strong magnet on the devices, which causes it to stop measuring usage, while still providing electricity to the customer[28]. This method is being used by some customers to disable the meter at night when air-conditioning units are operational. This is an example of the use of a physical attack that is related to a major concern in the power systems operation and planning, which is the existence of non-technical losses, also referred as commercial losses. This type of losses has consequences not only from the grid operational point of view, as it causes unexpected loads in system elements, but also from the economical point of view. Some works on non-technical losses' minimization and identification have been developed[29], but this stills an area to be improved while new data becomes available and suitable to be analysed by means of AI techniques. Anyway, these are also exampling on the concerns about security in smart grids.

[27] Warwick Ashford, "UK consumers fear cyber attacks on smart meters, survey reveals", April 2013. (Available on line in January 2014: http://www.computerweekly.com/news/2240182917/UK-consumers-fear-cyber-attacks-on-smart-meters-survey-reveals).

[28] Federal Bureau of Investigation, "Smart Grid Meters Altered to Steal Electricity", Intelligence Bulletin – Cyber Intelligent section", May 2010

[29] C.C.O. Ramos, A.N. de Souza, A.X. Falcao, J.P. Papa, "New Insights on Nontechnical Losses Characterization Through Evolutionary-Based Feature Selection," IEEE Transactions on Power Delivery, vol.27, no.1, pp.140-146, Jan. 2012

5.1 Cellular IoT Communication Technologies

Cellular IoT has been widely adopted across the globe, with 2G and 3G connectivity enabling many early IoT applications. Greater bandwidth, lower latency and increased support for large volumes of devices per cell are coming to the market with 4G offerings. These will be enhanced further with the arrival of 5G networks, initially enabled by the 5G New Radio (NR) standard, which will enable Ultra-Reliable Low Latency Communications (URLLC) that support increasingly critical applications.

Cellular IoT therefore has the capability to address both the relatively simpler requirements of the Massive IoT market as well as the highly specific, sensitive demands of complex environments and applications. The number of Cellular IoT connections enabled by Narrowband IoT (NB-IoT) and Long Term Evolution for Machines (LTE-M) continues to grow. The number of devices connected by Massive IoT and other emerging cellular technologies is forecast to reach 4.1 billion by 2024.

Cellular IoT itself is a rapidly growing ecosystem based on 3GPP global standards, supported by an increasing number of mobile network providers as well as device, chipset, module and network infrastructure vendors. It offers better performance than other Low Power Wide Area (LPWA) network technologies in terms of unmatched global coverage, Quality of Service, scalability, security and the flexibility to handle the different requirements for a comprehensive range of use cases.

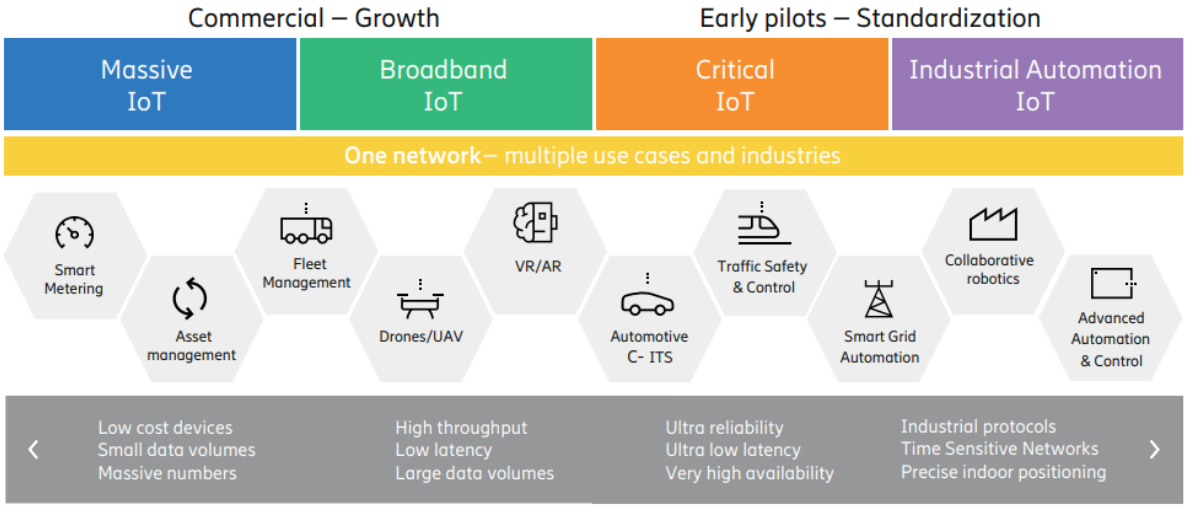


Figure 3. Cellular IoT Segments.

Broadband IoT adopts the capabilities of Mobile Broadband connectivity for IoT by providing much higher data rates and lower latencies than Massive IoT, while utilizing functionalities that are specific to Machine Type Communications (MTC) for coverage extension and extended device battery life. This segment targets a wide range of use cases in automotive, drones, Augmented Reality/Virtual Reality (AR/VR), utilities, manufacturing and wearables, based on 4G and 5G NR radio access technologies.

Critical IoT pushes the boundaries of Cellular IoT even further by enabling extremely low latencies and ultra-high reliability at a variety of data rates. This segment addresses extreme connectivity requirements of many advanced wide area and local area applications in intelligent transportation systems, smart utilities, remote healthcare, smart manufacturing

and fully immersive AR/VR. Powered by the most innovative capabilities of 5G NR, Critical IoT is expected to enable many new use cases within the IoT arena.

Industrial Automation IoT segment provides advanced Cellular IoT functionalities tailored for advanced industrial automation in conjunction with the other cellular IoT segments. It includes Radio Access Network (RAN) capabilities to facilitate the support of deterministic networks which, together with ethernet-based protocols and other industrial protocols, will enable many advanced industrial automation applications. These applications have extremely demanding connectivity requirements and require very accurate indoor positioning and distinct architecture and security attributes. Industrial Automation IoT reinforced by Critical IoT connectivity is the key enabler for the full digitalization of Industry 4.0 for the world's manufacturers, the Oil and Gas sectors as well as smart grid components for energy distribution companies.

With effective use of techniques such as network slicing and radio resource partitioning[30], all Cellular IoT segments can be supported in a single RAN allowing MNOs to optimize their assets and provide the best service to their customers.

Broadband IoT connectivity provides superior performance in terms of lower latency and higher throughput than the Massive IoT segment. Typical applications are advanced wearables, aerial and ground vehicles, AR/VR enabled devices and sensors that require greater capabilities than CAT-M or NB-IoT can provide. LTE has a range of device categories well-suited for such applications. For example, LTE is already providing cellular connectivity to millions of modern cars. There are LTE capable smart watches in the market and LTE-connected drones are coming next[31].

LTE offers high spectral efficiency and data rates, low latencies and has been enhanced with extended device battery life and improved coverage. With advanced multi-antenna solutions and carrier aggregation, LTE enables peak rates in the multi-Gbps range. Added to this, there are mechanisms for fast connection establishment and data delivery. With instant transmission schemes, the radio interface latency can be as low as about 10ms. The vendor specific LTE scheduler has advanced priority handling mechanisms to provide superior performance to a selected group of users.

Massive IoT connectivity targets huge volumes of low-complexity devices that infrequently send or receive messages. The traffic is often tolerant of delay and typical use cases include low-cost sensors, meters, wearables and trackers. Such devices are often deployed in challenging radio conditions such as in basement of a building. Therefore, they require extended coverage and may rely solely on a battery power supply which puts extreme requirements on the device's battery life.

3GPP standardized three new technologies for massive MTC in Release 13: EC-GSM-IoT, LTE-M and NB-IoT. LTE-M extends LTE with new features for improved battery life, extended

[30] Ericsson, "Network slicing can be a piece of cake", May 2018.

https://pages.digitalservices.ericsson.com/paper-network-slicing-can-be-a-piece-ofcake

[31] Drones and networks: Ensuring safe and secure operations. Ericsson White Paper:

https://www.ericsson.com/en/white-papers/drones-and-networks-ensuring-safe-andsecure-operations

coverage and support for low-complexity device category series, named CAT-M. NB-IoT is a standalone radio access technology based on the fundamentals of LTE that enables extreme coverage and extended battery lives for ultra-low complexity devices.

The radio coverage per base station is extended by means of repeating the transmissions, exploiting relaxed requirements on data rate and latency. A device can be allowed to sleep for extended periods of time with extended Discontinuous Reception (eDRX) and Power Saving Mode (PSM) functionalities, which significantly enhances its battery life. The complexity of CAT-M and NB-IoT devices is kept low by the utilization of narrow bandwidths, half-duplex operation and the incorporation of a single transmit-and-receive antenna on the device.

CAT-M devices have relatively greater capability and are more complex than NB-IoT devices. NB-IoT supports 200 kHz bandwidth, whereas CAT-M supports 1.4 MHz bandwidth with CAT-M1 and 5 MHz bandwidth with CAT-M2. Although CAT-M can operate in full-duplex mode, today's CAT-M ecosystem supports only half-duplex operation to limit device complexity and power consumption.

CAT-M and NB-IoT should target complimentary use cases. CAT-M is better suited for applications that require relatively higher throughput, lower latency, connected mode mobility, better positioning and voice connections. Typical CAT-M use cases include wearables, sensors, trackers, alarm panels and customer support buttons, all with support for data and voice connections. On the other hand, NB-IoT is the technology of choice for very low throughput applications that are tolerant of delay but require extreme coverage, such as simple utility meters and sensors deployed in challenging radio conditions. An additional advantage for service providers is that NB-IoT can be deployed in the guard-band of an LTE carrier making use of the spectrum that is otherwise unused.

CAT-M and NB-IoT are considered future-proof and seen as 5G technologies[32],[33]. They can efficiently co-exist with 5G NR in the same spectrum and already fulfil all 5G massive MTC requirements, as set out in the IMT-2020 and 3GPP standards, in terms of coverage, latency, data rate, battery life and connection density[34],[35]. CAT-M and NB-IoT are being further enhanced in 3GPP Rel-16.

[32] Evaluation of LTE-M towards 5G IoT requirements. GSMA:

https://www.gsma.com/iot/evaluation-of-lte-m-towards-5g-iot-requirements/

[33] Mobile IoT in the 5G Future – NB-IoT and LTE-M in the Context of 5G. GSMA:

https://www.gsma.com/iot/mobile-iot-5g-future/

[34] IMT-2020 self-evaluation: mMTC coverage, data rate, latency & battery life. Ericsson

and Sierra Wireless. 3GPP R1-1814144, Nov. 2018.

http://www.3gpp.org/ftp/tsg_ran/WG1_RL1/TSGR1_95/Docs/R1-1814144.zip

[35] LTE-M and NB-IoT meet the 5G performance requirements. Ericsson blog post, Dec.

2018. https://www.ericsson.com/en/blog/2018/12/lte-m-and-nb-iot-meet-the-5gperformance-requirements

In 3GPP Release 14/15, new features and enhancements have been made to the Massive IoT technologies Cat-M and NB-IoT. This includes important improvements in the areas of system capacity, performance and UE power consumption. It has been concluded [36],[37]. that both technologies fulfill the IMT-2020 [38], and 3GPP [39] requirements for a 5G system when using the Release 15 version of the 3GPP specifications. These fulfilled performance requirements are summarized below:

Connection density

At least one million devices per square kilometer (km2) shall be supported in four different deployment scenarios (as described in [39]) where each device transmits a small UL packet once every two hours.

Coverage

The coverage corresponding to a maximum coupling loss (MCL) of 164dB shall be supported.

Data rate

The sustainable uplink and downlink data rates shall be at least 160 bits per second (bps) at an MCL of 164dB.

Latency

An uplink packet of 105 bytes shall be received in the network within 10 seconds at an MCL of 164dB.

UE battery life

Ten-year battery life using a 5Wh battery for a traffic model will be achieved, with a daily delivery of an uplink message of 200 bytes followed by a 20-byte downlink message.

In addition to being key components of a 5G system, both Cat-M and NB-IoT can efficiently co-exist in the same band as an NR carrier. Dynamic spectrum sharing in the same band between all four technologies Cat-M, NB-IoT, LTE and NR are already supported in 3GPP

[36] 3GPP Tdoc R1-1907398 “IMT-2020 self-evaluation: mMTC coverage, data rate, latency & battery life”

https://ftp.3gpp.org/tsg_ran/WG1_RL1/TSGR1_97/Docs/R1-1907398.zip

[37] ITU-R, Report ITU-R M.2410-0, “Minimum requirements related to technical performance for IMT-2020 radio interface(s),” November 2017.

https://www.itu.int/pub/R-REP-M.2410-2017

[38] 3GPP TR 38.913 v15.0.0 “Study on Scenarios and requirements for next generation access technologies”

https://www.3gpp.org/ftp/Specs/2019-12/Rel-15/38_series/38913-f00.zip

[39] Ericsson, White Paper: Cellular IoT in the 5G era, January 2020

https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-in-the-5g-era

Release 15 and additional enhancements are being standardized as part of Release 16. This is being achieved (and still being further evolved) by: [40]

- a flexible NR numerology and frame structure compatible with LTE
- an NR frequency duplex configuration allowing NR, NB-IoT and LTE-M subcarrier grids to be aligned
- support for "forward compatibility" configuration, making it possible for NR user equipment (UE) to rate match around radio resources that are taken by non-dynamically scheduled NB-IoT and LTE-M signals

Cat-M and NB-IoT have a smooth and future-proof evolution in 5G networks when combined with dynamic spectrum sharing (DSS) features, a dual-mode core network solution (5G Core), and continued standardization in 3GPP. [41] [42]

5.2 Powerline Communication (PLC)

Power line communication (PLC) has been used by utilities for more than a century in many applications important for electricity services, protection as well as multiple purposes for transmission, distribution and last mile service providers.

PLC is a signal, emulated on the power sinus waveform and combining telecommunication and power delivery over the same wire from the plug. In some cases can be used in LAN application in house or wide area application for deliver data from and to the control center of the utility.

Smart grids do heavily use of ICT over the electrical power grid and therefore is changing the traditional way of serving the utility. The amount of data collected by more devices in field such as sensors, meters and actuators will enable a better understanding and control over the elements and bring a new knowledge domain to the utility operators.

5.2.1 Evolution of PLC

Using classical copper wires, PLC has been used since the last century mainly for voice and low data rate (bauds) data communication to manage and control power grid with Standards

[40] GSMA Mobile IoT report, January 2020

https://www.gsma.com/iot/mobile-iot-commercial-launches/

[41] GSMA Whitepaper, Mobile IoT in the 5G Future – NB-IoT and LTE-M in the Context of 5G, April 2018

https://www.gsma.com/iot/wp-content/uploads/2018/05/GSMA-5G-Mobile-IoT.pdf

[42] Ericsson, White Paper: Cellular IoT Evolution for Industry Digitalization, January 2019

https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-evolution-for-industry-digitalization

such as narrowband PLC for utilities (IEC 61334) in distribution level. Based on the reality that more data and speed is necessary, usage of broadband PLC have been introduced as well. Nevertheless, the good old world of FSK (Frequency Shift Keying) was no more good for utilities and new standards were introduced in late 90s and begin of 2000 based on OFDM (Orthogonal Frequency Division Multiplexing) .

Two huge breakthroughs in the development of PLC happen in the 1990s with the advent of broadband PLC (Broadband over Power Line or BPL). Initially, BPL was applied for Internet access (as an alternative to xDSL, HFC and radio systems), and still exists in the form of high speed devices for in-home communications which extend or replace Wi-Fi coverage. The second breakthrough came in the 2000s, with the application of PLC to smart metering, evolving from daily meter register reading to a close-to-real-time operation and management of low voltage elements, including connection and disconnection commands.

5.2.2 PLC and radio technologies

PLC in general is always seen as an alternative to radio technology for many utilities. Radio (wireless) is one of the most recognized telecommunication technologies and has many different applications. Radio is used in the low frequency spectrum range to cover distances of hundreds of kilometers for simple voice applications (commercial radio broadcasting). It is also used to provide broadband data services over public mobile telecommunication networks using the higher end of the spectrum.

PLC technologies behave like radio systems: frequencies are used to determine range. At the same time, the power grid is also a ubiquitous medium which reaches all smart grid endpoints. We can find ultra-narrowband PLC systems covering long distances and propagating through the grid with little attenuation due to grid elements. Found also, are narrowband PLC systems with low-data rates or high-data rates, depending on the underlying techniques (range will vary accordingly) and we can find BPL systems useful for a variety of applications and scenarios.

5.2.3 PLC for smart grid applications

PLC is ideal for smart grid applications, since a critical part of any network deployment is the infrastructure investment (cables and wires for wireline systems, repeaters, antennas and tower space for radio systems). This becomes crucial when we consider the kind of premises where smart grid services are to be provided. In the case of smart metering, devices are often located in cellars and even enclosed inside metal structures with no wireless coverage. Substations too require consideration as a significant percentage is, a significant percentage either in rural areas or underground, usually with limited access to wireline/wireless public telecommunication services.

PLC solves the problem by leveraging the electrical grid assets themselves. The solution for telecommunication services for smart grids requires utilities to define their requirements and goals, in terms of the evolution needs and the control strategy over their networks. This definition is related to a conceptual approach towards a smart grid that considers that the control of assets and their integration with the electrical infrastructure is as important as the asset themselves.

Once this definition is prepared, a deep knowledge is required both of the private utility's grid assets and of the possibilities of the public commercial services. This encompasses the theoretical capabilities of the services, the evolution of the technology supporting the network, the way the public telecommunication network is designed (reliability, resource sharing) and the real accessibility to the premises where the service is needed. All these factors are needed to understand the hidden costs of the services in the lifespan of the assets, and the percentage of the locations that will be effectively covered.

On the technical side, non-PLC wireline networks can easily become economically prohibitive if not deployed together with the electric grid assets (mainly power lines). Wireless networks present issues with spectrum availability and interference. Spectrum is usually available for specific smart grid purposes at a worldwide level; but if frequency is available, it could be very costly if opened up to a competitive bid process. License-exempt frequency bands are the only alternative when spectrum is not available. However, the transmit power limits imposed by regulation in these bands and their interference risks, deserve careful consideration.

PLC addresses the shortcomings of alternative private and commercial telecommunication solutions.

5.2.4 PLC in real deployments

PLC is deployed in hundreds of millions of smart meters and in-home devices worldwide. PLC systems have gone through a technical evolution so they can now be considered state-of-the-art telecommunications, both in the narrowband (ITU-T G.9901 to 9904 and IEEE 1901.2) and broadband (ITU-T G.9960, G.9961 and IEEE 1901) domains, for access and in-home. PLC is seen by utilities as a fundamental technology by the number of connected grid elements.

PLC is most commonly deployed in combination with other technologies. Different PLC options can be used for smart grid deployments: PLC in the low voltage grid and in-home for smart metering and home area network; PLC in medium voltage for smart grid backbone transport and tele control applications; PLC for remote high voltage grids where other means are not available; and so forth.

The PLC options listed above may be combined with other telecommunication private network or public commercial services, depending on the requirements and grid constraints.

5.3 Radio Frequency

Introduction of RF towards the electrical grid started with AMR (automated meter reading) solutions, formerly on walk-by or drive-by and nowadays on RF modem-based solutions within AMI (advanced meter infrastructure). AMI uses smart meters, whereas AMR is more dedicated to classical electronic meters or communication enabled mechanical meters (using of optical character recognition etc.)Smart meters, which operate by transmitting and receiving information wirelessly, are a key element in the effort to update and bring electric systems. Nevertheless, some consumers have expressed concerns about the possibility of negative health effects from the radio frequency (RF) waves that smart meters use to communicate.

5.3.1 What are radio frequency waves?

Radio frequency waves are a form of electromagnetic energy. They move through space at the speed of light and can be man-made or occur naturally. RF waves are used for a variety of purposes, but most importantly, they are employed in telecommunications. Smart meters use low-energy radio frequency waves to transmit information across distances.

Every day, people use and keep nearby to them many devices that utilize radio frequency waves, including microwave ovens and cellular telephones. In North America, the Federal Communications Commission (FCC) and in Europe CEN & CENELEC sets RF limits and requires that all radio communicating devices be tested to ensure that they meet federal standards before they are allowed to transmit within the radio spectrum. Smart meters emit less radio frequency energy than many other commonly-used wireless devices which, like smart meters, are safe and approved.

5.3.2 Using of RF for Smart Grids

Widely used in smart meters or electronical meters with communication environment (external and internal modem), RF is one of the most used solutions in case cellular network isn't present, PLC has an issue with interference and a reliable and fast solution is necessary.

Modems can be inbuild under the cable cover of the meter or connected through an RS485 interface towards and external modem for RF. Nevertheless the bandwidth will be limited due to the modulation scheme of the technology.

5.4 Cellular IoT Communications Security

NarrowBand-Internet of Things (NB-IoT) is a standards-based low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services. NB-IoT significantly improves the power consumption of user devices, system capacity and spectrum efficiency, especially in deep coverage. Battery life of more than 10 years can be supported for a wide range of use cases. New physical layer signals and channels are designed to meet the demanding requirement of extended coverage – rural and deep indoors – and ultra-low device complexity. Initial cost of the NB-IoT modules is expected to be comparable to GSM/GPRS. The underlying technology is however much simpler than today's GSM/GPRS and its cost is expected to decrease rapidly as demand increases. Supported by all major mobile equipment, chipset and module manufacturers, NB-IoT can co-exist with 2G, 3G, and 4G mobile networks. It also benefits from all the security and privacy features of mobile networks, such as support for user identity confidentiality, entity authentication, confidentiality, data integrity, and mobile equipment identification. [43]

6 Smart Grids Cyber-Physical Security

Cyber-physical attacks on critical infrastructure that have the potential to damage those physical assets and to cause widespread losses to own valuable systems. A cyber-physical attack on critical infrastructure occurs when a hacker gains access to a computer system that operates equipment in a manufacturing plant, oil pipeline, a refinery, an electric generating plant, or the like and is able to control the operations of that equipment to damage those

[43] https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/

assets or other property. A major cyber-physical attack on critical infrastructure is a risk not only for the owners and operators of those assets, but also for their suppliers, customers, businesses and persons in the vicinity of the attacked asset, and any person or entity that may be adversely affected by it (e.g., consumers and shareholders). [44]

If the cyber-attacks in the worldwide are reviewed. Based on the WORLD ENERGY COUNCIL report from 2016, a recorded cyber-attacks against energy sector between 2003 and 2015, cyber-attacks took place in many countries, especially in the USA, Israel, Ukraine, the Netherlands and Saudi Arabia.

Supervisory control and data acquisition (SCADA) systems are highly distributed systems used to control and monitor geographically dispersed assets-often scattered over thousands of square kilometers-in which centralized data acquisition is critical to system operation. These large-scale industrial control systems have been playing an extremely important role in most safety-critical infrastructures, such as electric power grids and communication networks. These safety-critical assets, however, are becoming increasingly susceptible to cyber-physical attacks on both physical and cyber layers. [45]

Unlike all these cyber-attacks, there have been only two major publicized cyber-physical attacks. The first was the use, in 2008 through 2010, of the Stuxnet virus to destroy approximately 20% of Iran's centrifuges used to make nuclear materials. Stuxnet reportedly damaged the centrifuges by causing them to spin out of control. In the second attack, in late 2014, the hackers gained access to the computers of a German steel mill through a minor support system for environmental control. The attack led to the destruction of a blast furnace in the steel mill. German authorities did not allow the publication of many details of the attack, but they did describe the resulting damage as "massive."

While cyber-security has emerged as a very IT-focused discipline when interconnection of local networks to the internet became a standard, we acknowledge now that the "machine to machine" communication, and particularly the adoption of smart grids get more and more entangled. Hence the emergence of a concept of "cyber-physical system" embracing on SCADA, Industrial Automation and Control Systems (ICAS), Smart grids but also embedded command & control systems and the Internet of Things (IoT).

Cyber-physical attacks, also called blended attacks, are executed by an adversary or result from inadvertent action. Cyber-physical attacks can be classified into three broad subsets:

Physical attacks informed by cyber – The use of information gathered by cyber means that allows an adversary to plan and execute an improved or enhanced physical attack.

Cyber-attacks enhancing physical attacks – An adversary uses cyber means to improve or enhance the impacts of a physical attack by either making the attack more successful or interfering with restoration efforts.

[44] http://www.klgates.com/cyber-physical-attacks-on-critical-infrastructure--whats-keeping-your-insurer-awake-at-night-01-24-2017/

[38] https://ieeexplore.ieee.org/document/7954148

[38] https://www.gsma.com/iot/narrow-band-internet-of-things-nb-iot/

Use of a cyber system to cause physical harm – An adversary uses a cyber system that controls physical equipment in such a manner to cause physical harm/damage.

A major limitation though is that the security of a cyber-physical system cannot just be tackled by adding physical security at operational technology level and cyber-security at IT level. A new federative approach is required to assess impact of cyber-incidents and countermeasures on grid operation and processes, to identify vulnerabilities of state-of-the-art SCADA protocols in use and to identify the most likely attack scenarios in this particular environment.

Nations are dependent on the reliable functionality of critical infrastructures, such as electrical, gas and water grids. Major concerns have been highlighted in documents such as "Smart Grid Cyber Security Potential Threats, Vulnerabilities and Risks", from the California State University Sacramento[46], the NIST "Guidelines for Smart Grid Cyber Security[47], and at the European Smart Grid Standards[48].

In the references to the cyber security framework published by NIST, the system architecture was examined in a hierarchy consisting of five steps to provide the security of a system and information and suggestions were made for the solution of all events in the architecture through this hierarchical order. The block diagram showing these five steps is given in Figure4. If these steps are listed;

1. Identify: To establish a corporate understanding to manage the cyber security risk, to be able to list the definitions of cyber security risks in detail and functionally.

2. Protect: Develop and implement preventive services for critical and priority infrastructure services (Authentication and Access Authorization, Data Security, End-user training, Information Security Processes and Procedures, etc.)

3. Detect: Establishing software and hardware mechanisms that can reveal security vulnerabilities and attacks to the system during operation.

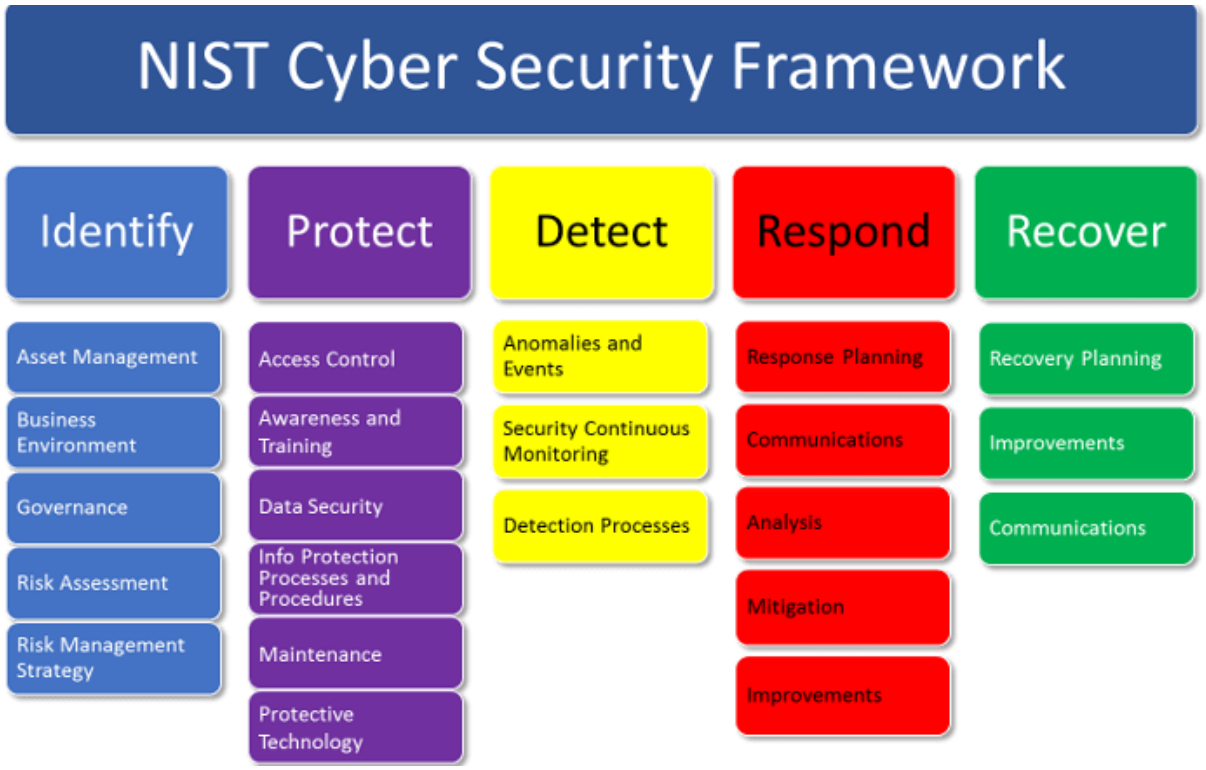
4. Respond: Designing the infrastructure that will produce the fastest response to a problem, anomaly or an attack occurring in the system, and ensuring that the processes in the response mechanisms of the system operate in a way that causes minimal damage to other units.

5. Recover: To create the infrastructure that will enable the system to repair the security problems that occur in itself and return to the latest healthy working conditions as soon as possible.

[46] http://www.energy.ca.gov/2012publications/CEC-500-2012-047/CEC-500-2012-047.pdf

[47] http://dx.doi.org/10.6028/NIST.IR.7628r1

[48] http://www.smartgrids.eu/standards



Preventing cyber-attacks on energy transmission and distribution systems and especially end users is an increasingly important issue. Different methods may be required to prevent security vulnerabilities of SCADA-like systems used in smart grids and to protect these systems from attacks. It may not always be possible to test applications on real systems to protect systems from physical cyber-attacks and cyber-attacks. Therefore, the creation of smaller demonstration areas to simulate attack and loss and leakage scenarios and the implementation of different scenarios in these demo areas may yield faster results in finding solutions. In this way, cyber-attacks and physical cyber-attacks can be defined in order to find and develop quick solution methods.

6.1 Smart Grid Communications Security

Smart grids applications are typically based upon client-server architecture and security of those applications is primarily addressed to secure point to point communication between the gateway and applications servers.

The role of the M2M service platform appears known as a key component to insure interoperability between heterogeneous applications. Such a platform offers a number of services which simplify the coding of M2M applications, and more specifically it enables a dynamic definition of the data flows.

Furthermore, efforts have been undertaken by standardization bodies such as IETF, ETSI (now ONEM2M) to define standards for interoperable M2M service platforms. However, with the advent of M2M services platform, the communication model evolves from a point to point client server model towards a point to multipoint peer to peer communication model.

From the security standpoint, the management of credentials used to secure M2M applications has been fairly static, and this also, needs to evolve: The problem is not

anymore to secure the communication from devices to application server, but rather to secure communications from devices to every single application needing and authorized to interact with devices.

Authentication and data protection issue are commonly addressed by M2M applications, but Authorization is seldom addressed, and this is regrettable. Fine grained authorization management is an essential component of a secure architecture, enabling to define precisely which applications may to interact with one device and in which way.

Also, the implementation of a security scheme is always associated to the distribution of credentials. Protecting the storage and use of those credentials is essential to avoid compromising the security. The problem is challenging on the device side where the theft of credentials opens the way to device cloning. Secure elements offer a proven solution to protect the storage of credentials in embedded appliances. Their enrolment and the management of the credentials stored in their memory is performed using specialized secure element management platforms which have been traditionally operated by the business entities issuing the secure element such as telecommunication or payment companies. But recent years have seen the emergence of the notion of “security domain” enabling a single secure element to be exposed as a shared platform used by independent service providers.

The underlying business model involves the secure element issuer to “lease” secure element space to third parties’ providers for them to remotely store and manage their own credentials in their private secure space. This model could apply to smart grids and smart grid devices as it opens the possibility for multitenant administration of the credentials stored in the devices and it supports emerging business models for smart grid operation.

This idea of multitenant administration has initially emerged to enable multiple providers to offer mobile services requiring strong security for client-side credentials. Unfortunately, the energy efficiency involved for mobile applications are extremely diverse and sometimes very complex compared to IoT and more specifically smart grid use cases.

The need to support a large variety of use cases configurations has a very significant impact in the cost of the process to remotely manage the credentials on the secure elements. Although mobile and IoT vertical domains share the same initial idea of multitenant secure element administration, different solutions should be used in each of those market segments, and simple and cost effective secure element solutions are needed to make possible wide deployment.

Intrusion detection system (IDS) acts as a second wall of defence and is necessary for protecting AMI if security mechanisms such as encryption/decryption, authentication and etc. are broken. Intrusion detection is the process of monitoring the events occurring in a computer system or network and analysing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Generally, techniques for intrusion detection are classified into three main categories: (i) Signature-based, (ii) Anomaly-based, and (iii) Specification-based. While efforts have been made to investigate the security of AMI, there are a few works that focus on proposing and designing reliable and efficient IDS for AMI.

7 Standards

Smart Grid networks yield their full potential benefits when based on open standards. Standards enable interoperability, which in turn ensures that the broadest possible set of products work together. There are hundreds of standards for Smart Grid that have been developed in parallel by different organizations. For smart grid, there are over 25 standards development organizations involved in updating and developing standards, for example, IEC, IEEE, IETF, ISO, ITU, NAESB, NEMA, SAE, and many more.

IEEE (2,500 papers in over 40 IEEE journals) has nearly 100 standards and standards in development relevant to smart grid, including the over 20 IEEE standards named in the NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0. The NIST report describes a high-level reference model for the smart grid, identifies nearly 80 existing standards and high priority gaps for which new or revised standards are needed[49].

In [50] it is possible to find and easily understand the fundamental standards of Smart Grid. The authors highlight the most advanced works such as the "NIST Framework and Roadmap for Smart Grid Interoperability Standards Release 2.0", the "IEC Smart Grid Standardization Roadmap", the ISO/IEC's "Smart Grid Standards for Residential Customers", the ZigBee/HomePlug's "Smart Energy Profile Specification 2.0", and the IEEE's P2030 "Draft Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), and End-Use Applications and Loads".

Some of the standards to consider include:

- IEC 62351 – 1 to 7 standards for Data and communications security
- IEC 61850 – 1 to 10standard for Communication networks and systems in substations
- ISO/IEC 27001 standard for Information Security Management System
- ISO/IEC 15408 -1/2/3 Security techniques -- Evaluation criteria for IT security
- IEEE SCC21 1547 Interconnecting Distributed Resources with Electric Power Systems
- IEEE 762 Use in Reporting Electric Generating Unit Reliability, Availability, and Productivity
- IEEE SCC 31 standard for Automatic Meter Reading and Related Services
- IEEE 802 LAN/MAN Standards Series

The NERC Critical Infrastructure Protection (CIP)[51] plan consists of 9 standards and 45 requirements covering the security of electronic perimeters and the protection of critical cyber assets as well as personnel and training, security management and disaster recovery planning.

- CIP-002-1: Critical Cyber Asset Identification

[49] http://smartgrid.ieee.org/ieee-smart-grid

[50] Takuro Sato, Daniel M. Kammen, Bin Duan, Martin Macuha, Zhenyu Zhou, Jun Wu, Muhammad Tariq, Solomon A. Asfaw, "Smart Grid Standards: Specifications, Requirements, and Technologies", IEEE Press, Wiley, to be published (overview available at www.wiley.com).

[51] www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

- CIP-003-1: Security Management Controls
- CIP-004-1: Personnel and Training
- CIP-005-1: Electronic Security Perimeters
- CIP-006-1: Physical Security of Critical Cyber Assets
- CIP-007-1: Systems Security Management
- CIP-008-1: Incident Reporting and Response Planning
- CIP-009-1: Recovery Plans for Critical Cyber Assets

8 Software Defined Networks based Smart Grid

SG (Smart Grid) needs continuous information exchanges between smartmeters and AMI (Advanced metering infrastructure), this information need to be conducted through a secure and reliable communication system and need to be managed globally[52].

Multi packet label switching (MPLS) has been adopted by the utilities for smart grid communication system but this is based in routers that need to be re-configured each time, disrupting the services provided by the utilities[53].

The alternative is SDN (software defined networks), that monitor and manage the communications networks globally. SDN has already been applied to different domains.

For SG, SDN can be the base for SG communication support and to manage the communication entities in the SG system, improving efficiency and resiliency.

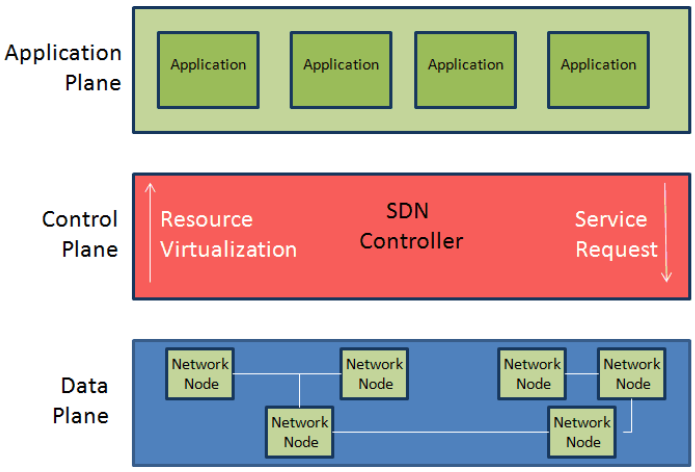
The SDN-based SG can be used for load balancing and shifting, for dynamically adjusting the routing paths for SG control commands, fast failure detection, security, self-healing and for monitoring and scheduling of critical SG traffic flows.

Actually main issues with SG are security and privacy. Also, Network management of current SG systems is complex, time consuming, and done manually. This also includes manual intervention from the network administrators and network engineers to configure and implement the policies in each device, so it isn´t enough flexible[53].

As traditional networks aren´t programmable, the need arises of programmable networks. SDN separate the hardware from the control decisions, so network devices become forwarding devices and the software defined controllers leds the network intelligence. This way it gains enormous programmability, automation and control of the network, allowing to build networks highly scalable and flexible, which They adapt quickly to the requirements of the business areas. With SDN get independence and control over all the network infrastructure from a single logical point, simplifying the design and the operation. SDN also simplifies network devices, because they don't have to process hundreds of standard protocols. They should only accept instructions from SDN controllers.

[52] Ramyar Rashed Mohassel, Alan Fung, Farah Mohammadi, Kaamran Raahemifar, A survey on Advanced Metering Infrastructure, International Journal of Electrical Power & Energy Systems, Volume 63, 2014, Pages 473-484,

[53] Mubashir Husain Rehmani, Alan Davy, Brendan Jennings, and Chadi Assi, Software Defined Networks based Smart Grid Communication: A Comprehensive Survey (January 2018) (arXiv.org > cs > arXiv:1801.04613v4)



Basic architecture model of software-defined networks

SDN takes advantages of many functionalities and access to fine grained packet related information through SDN controllers, such as OpenFlow and OpenDayLight. This information help the SDN controllers to access packet collision related information, port information, hardware description, and the type of connection used. Moreover, SDN controllers are capable to dynamically configure the flow entries on switches and routers. SDN controllers can also identify errors in data paths, unidentified packets, and may remove or alter the data flow path entries[54].

Most used protocol of SDN communications is OpenFlow Protocol which allows the software serve to determine the path of packet forwarding that it shoud follow in a switch network. With the OpenFlow protocol, a network can be managed as a whole, not as a number of devices that are managed individually, it is the server itself that gives the switches where they should send the packets.

Use SDN-based SG has different advantages over traditional networks:

- As different types of traffic are generated by different devices in a Smart grid. Using SDN in Smart Grid different traffic types or applications can be isolated.
- In a smart grid there may be measurements data and control commands that could have high priority. SDN can prioritize the traffic flexibly.
- SDN can help to create virtual network slices in the smart grid.
- SG Resilience – Resilience is the ability of the SG system to react with failures and attacks and in response to these failures and attacks, SG should recover and maintain its critical services. SG will become more reliable by directing traffic flow from broken wired links to wireless link, Smart grid got more resilience.
- Quick fault detection. With SDN, SG achive fast link failure recovery by routing the packets to a alternative route without consulting to the SDN controller when a communication link fails.

[54] Carlos Spera; Software Defined Network: el futuro de las arquitecturas de red; (March, 2013) Logicalis Now.

- Fault tolerance improves with SDN, fault tolerance is the ability of the SG system to sustain operating properly even in the presence of a fault.
- Timely shifting the line load may prevent voltage collapse in SG. Also, SDN controller can select less overloaded links to prevent congestion issues over the links.
- Different types of communication network devices can be managed and configured to interoperate each other
- SDN improves run time configurability
- Network management become easier. It doesn´t requires manual intervention.

8.1 Security of SDN-based Smart Grid

Smart grids are critical infrastructure and they should be resilient under malicious attacks situations or when accidental failure occurs.

The SDN architecture can be improved to improve network security with the provision of a highly reactive security monitoring, analysis and response system. The central controller is a key part for this system. Traffic analysis or anomaly detection methods by means of probes implemented in the network, security related data, which can be frequently transferred to the central controller. Applications can be run on the controller to analyze and correlate this network data. Based on the analysis, the new or updated security policy can be propagated through said network controller in the form of flow rules. This consolidated approach can efficiently accelerate the control and containment of red threats and their security.

However, the same attributes of centralized control and programmability associated with the SDN platform present network security challenges. A greater potential for Denial of Service (DoS) attacks due to the centralized controller and the limitation of the flow table in network devices is a perfect example. Another issue of concern based on the open programmability of the network is trust between applications and controllers, and between controllers and network devices. Several solutions to these SDN security challenges have been proposed in many academic and great professional texts, where they range from controller replication schemes to resolving policy conflicts and authentication mechanisms.

Due to the nature of the centralized controller and the programmability of the network, new threats are introduced that require new responses. A series of techniques are proposed to approach the various threats, including replication, diversity and safe components.

SDN security needs to be built into the architecture, as well as delivered as a service to protect the availability, integrity, and privacy of all connected resources and information.

Some points to consider into the architecture are: The access to the SDN controller as the centralized decision point must be very controlled. If the SDN Controller goes down, so goes the network, which means the availability of the SDN Controller needs to be maintained. SDN controller, applications and devices must be trusted to protect the communications throughout the network. Have a robust policy framework and determine what happens when an incident occurs to protect against it in the future.

9 Related Projects

We would like specially to put the focus on SEAS. Indeed, this project consortium has several partners in common with SECUREGRID. The SEAS (Smart Energy Aware Systems) ITEA 2 project is to enable interactions for all market players in real time for consumption and production energy systems, automation and ICT Information and Communications Technology systems in order to optimize global energy consumption. An analysis of SEAS use cases will be done in WPs SecureGrid Scenarios, SecureGrid Architecture and Grid Security.

Link to previous and/or current collaborative research projects:

Project Name	Cooperative Programme	Time period (approx.)	Technical Focus	Relationship
SEAS: Smart Energy Aware Systems	ITEA2	Feb 2014 - Dec 2016	SEAS address smart energy aware systems in building and micro-grid environments.	Cybersecurity is a concern for SEAS. SecureGrid may test and implement cyber security approaches extending SEAS platform.
ADAX: Attacks Detection And Countermeasures Simulation	ITEA2	Jan 2013 - Apr 2015	ADAX aims to study feasibility of solutions enabling to detect complex attacks against an information system working in its complex environment and to react smartly and quickly to those attacks with adapted countermeasures.	SecureGrid may extend the concepts for the electricity networks.
ENERFIENCY User Led Energy Efficiency Management	ITEA2	Dec 2011 - Oct 2014	Open platform for industrial plants, large scale buildings and citizens for the optimization of energy consumption and the definition of business models for energy savings.	SecureGrid may extend the platform to address security vulnerabilities and how to prevent, detect and respond to them.
IMPONET Intelligent Monitoring of Power Networks	ITEA2	Dec 2010 - Mar 2013	Research, definition, design and development of new generation IT platforms for energy management and	SecureGrid may extend the IMPONET platform with security approaches for both remote management and

	network optimization.	monitoring.

Table 1: Related collaborative research projects.

The previous table gives just a short overview on the huge number of projects that have been developed within the last years. The JRC's 2013-14 Smart Grid database[55] contains 459 smart grid R&D and Demo & Deployment projects from all 28 European Union countries, launched from 2002 up until today, which amount to €3.15 billion in investments.

In the last JRC report on "Smart Grids Projects Outlook 2014" we can learn about all the European projects aimed at making the grid smarter through new technologies (e.g. storage devices, electric vehicles, distributed renewable generators) and new ICT capabilities. Looking at the analysis of the projects applications by category some conclusions are also drawn about areas of improvement, and this are standardization and interoperability, particularly on the communication infrastructure, and on cyber security.

SecureGrid emerges as covering one of the areas of improvement pointed out by JRC report, cyber security in smart grids, and in extending previous and related ITEA projects, namely SEAS, ADDAX and WATER-M.

10 Proposed technological innovation and novelty in relation to the SotA

The potentiality of NNs to be applied to a large variety of complex problems in very distinct fields makes this technology a promising tool to approach several issues of SecureGrid that require solid predicting capabilities. SecureGrid will use existing NN based technologies to predict malfunctions in the grid and prevent that failures cause a high impact. Additionally, innovative, enhanced and domain directed forecasting methodologies will be proposed, based on NN derivative branches (such as Support Vector Machines, Self-Organizing Maps NN, Fuzzy Inference Systems, Deep Learning, among others).

The used and developed forecasting methodologies will also be applied to the prediction and detection of security breaches or potential attacks. Additionally, the NN based forecasting methodologies will also be used to predict the spread of distributed generation, demand response participation and other customer-side changes to meet regulators' requirements to build these expectations into future distribution grid plans, in order to prevent problems that may arise in the future, if networks are not prepared for the expected changes.

Forecasts will provide the basis for preventive or reactive actions to be taken. These actions will be performed automatically, using machine learning methodologies to learn the best ways to act in each given context. E.g. when network faults are predicted or detected, different types of alerts must be launched depending on the gravity and impact of the failure; additionally, a sensor network reconfiguration can be necessary, and in that case, this should be defined as quickly as possible.

While characterization of consumers' profiles has been an active area of research within the last years, in this project advances in consumers' characterization will be used to create methodologies that automatically perceive abnormal consumption profiles, with the objective of detecting eventual cases of non-technical losses and fraud.

[55] ses.jrc.ec.europa.eu

For power systems operation and planning the correct estimation of actual system conditions is crucial. There are several sources of uncertainties being some of them resultant from electricity theft by consumers, other resultant from the unexpected losses in the system elements, the variable production from renewable sources, the weather conditions, etc. SecureGrid will use Big Data and Artificial intelligence techniques to develop new alternative and flexible methods to estimate system actual conditions. On one hand clustering and classification will be used to define system patterns according to the context and on the other hand, based on intelligent algorithms such as Artificial Neural Networks, Support Vector Machines, Nearest Neighbours, Fuzzy Logic, among others, to estimate the actual system conditions.

There are already developments in methodologies for the intelligent management of smart grids and microgrids, usually seen as smart grids building blocks in a particular localization. These methodologies should be improved in order to accomplish the effects of distinct types of attacks and the evaluation of the specific countermeasures. This may be done by means of simulation techniques that evaluate different attacks combined with different countermeasures. In this context machine learning will improve the decision support tools by learning the effect of the attacks according to specific contexts.

While cyber-security has emerged as a very IT-focused discipline when interconnection of local networks to the internet became a standard, we acknowledge now that with the “web of objects” revolution, the “machine to machine” communication, and particularly the adoption of smart grids in the energy domain, information technology and operational (OT) technology get more and more entangled. A major limitation though is that the security of a cyber-physical system cannot just be tackled by adding physical security at OT level and cyber-security at IT level. A new federative approach is required to assess impact of cyber-incidents and countermeasures on grid operation and processes, to identify vulnerabilities of state-of-the-art smart grids protocols in use and to identify the most likely attack scenarios in this particular environment. Therefore, a particular innovation outcoming from this project will be the development of a cyber-physical system simulator to support grid security operator in assessing attack impact and selecting the most appropriate countermeasures.

One of the main novelties will be to use Big Data Analytics, machine learning and artificial intelligence on extreme large datasets for critical grid infrastructures.

11 Conclusions

Throughout this document the state of the art of the major technologies that have been applied or considered for the realization of the project has been shown. The document is based on the three main pillars of the project, namely, Smart Grid, communications and security. This document is a landscape of all the main techniques and technologies in the field of the project, but also a tool to understand what are the novelties proposed by Securegrid and their potential impact in the sector and the society.

12 References

Carlos Spera; (March, 2013) Software Defined Network: el futuro de las arquitecturas de red; Logicalis Now.

Rehmani M.H., Davy A., Jennings B., Assi Ch. (January 2018) Software Defined Networks based Smart Grid. Communication: A Comprehensive Survey

Mohassel R.R., Fung A., Mohammadi F., Raahemifar K., (2014) A survey on Advanced Metering Infrastructure, International Journal of Electrical Power & Energy Systems, Volume 63, Pages 473-484.