DOI: 10.1051/matecconf/201712503011

# Considerations for IP Interconnection of Power Grid Components

*Velissarios* Gezerlis[1], *Maria* Belesioti[1,*], *Tilemachos* Doukoglou[1], *Ioannis* Chochliouros[1]

[1]Hellenic Telecommunications Organization S.A. (OTE), 1, Pelika & Spartis Street, 15122 Maroussi-Athens, Greece

**Abstract.** The foreseen capabilities of 5G, such as reliable and robust handling of data management can be commonly utilized by different sectors. The Electricity sector has remained for many years a stable industry using the same operational and maintenance regimes and dependable infrastructure. The need to integrate communication network domains in the Smart Grids context with 5G is considered as the next generation regarding power grids, and it is bidirectional as far as electricity and information is concerned, aiming to create a widely distributed automated energy delivery network (as in [1]). In this paper, a Communication-as-a-Service scenario is presented as a proposal of a telecom operator in order to “address” scalability, security and interoperability that a Smart grid network requires, by using communication solutions provided by 5G.

## 1 Introduction

Back in 2007, National Institute of Standards and Technology (NIST) has been assigned to coordinate the development of a framework that includes protocols and model standards for information management, based on research that has been previously made so as to create frameworks flexible, uniform and technology-neutral, able to achieve interoperability of smart grid devices and systems 2. The electrical power supply started more than a century ago with decentralized isolated networks, and has been evolved to a European centralized mixed network. Since the beginning of the 21st century, more and more decentralized energy systems are being introduced into the network again, so future architectures will have to support both centralized and decentralized concepts 3. Nowadays electricity constitutes the most versatile used form of energy and its demand is growing continuously, in a global level. Traditional electrical power systems delivering energy to commercial and residential consumers are about to exceed their limits.

Smart grids can “meet” the need of the ever-growing demand by combining communications and information technology with production, delivery and consumption of electrical energy and, *at the same time*, by improving system’s reliability and stability without increasing maintenance costs.

This paper is organized as follows: Section II introduces the general idea of distributed energy systems and the proposed overlay network architecture. Also the model of the proposed scenario is presented, by using the SGAM (Smart Grid Architecture Model) tool. Section B briefly describes VPN (Virtual Private Network) technology and the deployment of a VPN network in this scenario, as well as the IPsec protocol suite. Section III is referred to the usability of 5G networks in the Smart Grid Sector. Finally, Section IV contains the relevant conclusions.

## 2 Development of a complete simulation environment

Distributed energy systems have a great role to play and will have a huge impact on future electrical supply systems as well as lead to many financial benefits. Up to now, energy systems are integrated into electric grids. Special designed topologies and/or control for almost each particular case is required, which means waste of money and time for debugging **Error! Reference source not found.**. *The SmarterEMC2* H2020 EU-funded research effort under Grant Agreement No.646470 proposes the implementation of ICT tools that support Customer Side Participation and Renewable Energy Sources (RES) integration and facilitate open access in the electricity market. The consumers would be part of the scheme through an advanced Demand Response system that will be able to manage consumption and effectively communicate in a multi-level hierarchically organized Smart Grid, involving other entities as well as, *for example*, ESCOs (Energy Services Companies).

From the ICT point of view, smart grids involve the integration of an information infrastructure with the existing power systems (generation, transmission and/or distribution physical systems). This integration arises from the need of a more advanced level of automation in the Smart Grids, when compared to existing grids of today and will require the deployment of a vast telecommunication infrastructure leading to the

[*] Corresponding author: mbelesioti@oteresearch.gr

increased introduction of ICT in the power grids. The main goal in the area of Smart Grids is to create a complete-simulation environment (encompassing Power & Communication infrastructures) to evaluate the implementation of different distributed algorithms, advanced grid control policies and their performance in near-real life conditions. Initially, the time restrictions and/or limitations imposed by the communications' infrastructure will be identified, by creating heavy data applications related to the power grid operation, such as power quality indices and billing.

Additionally, applications based on reliable two-way communications to gain access to the data of smart meters and other measurable components of the power grid will be performed. More specifically, control commands will be sent to various appliances, after ensuring that they are ready to accept commands, in order to implement the smart control operations of the power grid and gain access to detailed measurements, regarding the impact of these operations on the power quality.

For the power grid so far classic simulated operations -such as the state estimation or the reconfiguration of the power grid structure according to the real condition of the system- are getting different importance and meaning, due to the deployment of telemetry projects and the installation of smart meters and other devices capable of storing data and communicating as often as it is required.

Furthermore, the need for more hosting capacity of renewable resources dictates the need for supervising "more closely" the power grid, in order to avoid the power quality loss, as well as the need to be able to issue control orders and implement distributed algorithms on the power grid actors to "maintain" the balance.

The effectiveness of such control schemes has to be proven within the framework of the telecommunication technologies to be used in two different time scales. Specifically, we should examine the minimum telecommunication requirements (round-trip delay, bit rate, reliability, QoS – as well as impact of failures and failover to backup routes) to obtain an acceptable level of management over the power grid in near real-time applications, by measuring the upper limit of the information required to be exchanged. On the other hand, we should also define the threshold of time resolution for facilitating appropriate applications, which are requiring the exchange (mainly one-way communications) of huge amount of data in an "offline" mode (i.e.: store and forward operation).

The integration of these technologies facilitates convergence of standards and implementation of necessary analytical capabilities. SmarterEMC2 proposes a system which will stand as an overlay communication network for the interconnection of the Power Grid elements (off-net management). During the past years, this type of network has evolved as the most commonly used way to share data and services, among a network of loosely connected components 4.

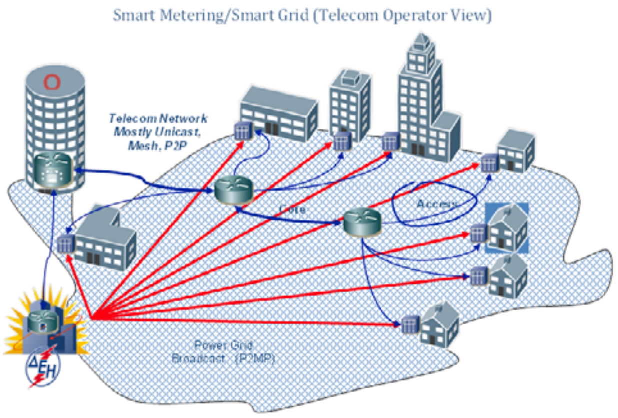

**Fig.1:** Smart Metering (Telecom Operator View)

This overlay communication system, as far as transmission is concerned, can be either wireless using LTE, 3G and GPRS or wired (copper cable and/or fiber optics). At this point, it should be clarified that the above mentioned communication system is divided into two major networks, that is: home network and Wide Area Network (WAN). As far as the latter is concerned, SmarterEMC2 will use the already broadband (wired/wireless) network of the telecommunication operator participating in the project, in order to establish communication between home networks, ESCOs and power generators (see Fig.1). Home network will be the one having direct impact to the consumer, since it is located inside his house. ZigBee protocol is the one that will most probably be used for the deployment of this kind of network. ZigBee is a specification for small, low power radios based on *IEEE 802.15.4 – 2003 Wireless Personal Area Networks standard* **Error! Reference source not found.** and is considered ideal for energy monitoring and home automation 6. In the following scheme (as in Fig.2), the modelling of communication layer is presented.

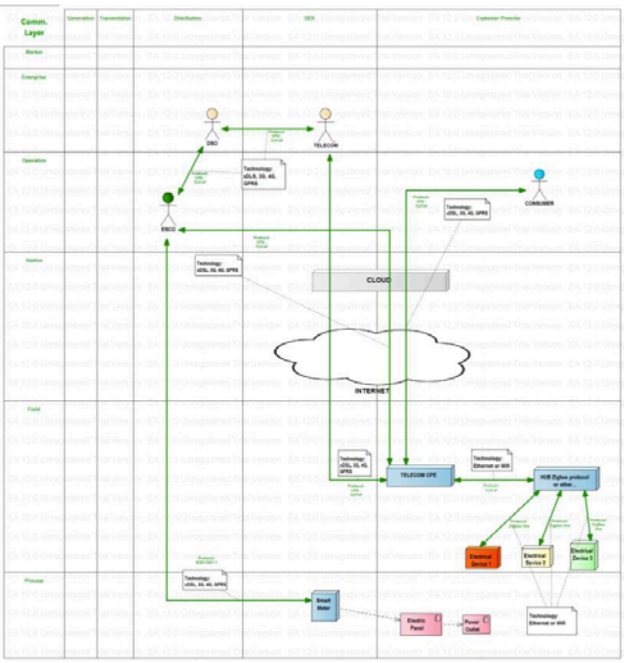

**Fig. 2**: Modelling of Communication Layer

Smart grid is a complex system, consisting of many processes and levels both in the area of energy and in the communication field. The connections among the electrical and telecom equipment are imprinted along with the relation among consumers, telecom operators and DSOs (Distribution System Operators). All, protocols that will be used as well as the home network and the WAN are described thoroughly in this SGAM model.

The above depicted communication layer is divided into zones and domains. In the vertical axis, the TelCo's communication system uses all zones, except for the market. Every actor of the horizontal domain should correspond to the vertical zone. Thus, in the distribution and DER (Distributed Energy Resources) domains and enterprise zone, DSOs and telecom operators are listed. Energy service companies have operational role and are responsible for distributing energy so are corresponded to the specified point.

As far as the customer premises domain is concerned, all telecom and electrical equipment is located. More specifically, all electrical physical equipment (outlets, electric panels, etc.) are in the process zone and all physical communication equipment are in the field zone. Home electrical devices, through *ZigBee Protocol* will send signals/messages to ZigBee Hub, which also will be located inside the house. By using Ethernet or/and WiFi the information will be transferred to operator's CPE (Customer-premises equipment) and then through separated VPNs each of the actors will be able to have access to the information. The technology used for this final transmission can be either wired (e.g. xDSL) or wireless (3G/4G). Internet Protocol (IP) will be used and different means of access depending on availability and traffic demand -such as Copper and Optical Fiber- will be utilized. One or more VPNs will be created for communication between the "energy/utilities" grid elements, with respect to the privacy and security of the data and "grid elements" using cryptography and Tunnel connections (i.e., Internet Protocol Security (IPsec)).

## 2.1 VPN deployment

IP-*based* user applications are becoming increasingly popular and the Internet technology has emerged as the major "driving force" behind new developments in the area of telecommunication networks. In an environment where clients are connecting to ever-growing networks, security requirements are of high importance. VPNs have become the logical solution for remote-access connectivity, since they provide secure communications with access rights tailored to individual users, such as employees, contractors or partners, and with reduced communications costs and increased flexibility. In remote-access VPNs, deployment can use two primary methods: IP Security (IPsec) and Secure Sockets Layer (SSL), each one with its advantages mainly based on access requirements needed. In the specific case of the *Communication-as-a-Service* deployment, the related VPN deployment is based upon the IPsec protocol suite, a developing standard for security at the network or packet processing layer. It provides encryption and integrity protection of packets on both IPv4 and IPv6, as well as authentication of the communicating entities.

VPNs allow for private data to be transmitted securely over public networks. They can also offer enormous versatility and customizability through modification of the VPN client software. Besides security, VPNs encompass an entire spectrum of technologies such as quality of service (QoS) and network management (NM). IPsec allows secure communication, by using authentication and encryption in each IP packet of a session. It provides encryption on IPv4 and IPv6, as well as authentication of the communicating entities.

IPsec grants two choices of security service: Authentication Header (AH) 8 where it provides data origin authentication, but does not provide secrecy, and; Encapsulating Security Payload (ESP) 9, where confidentiality is supported and data origin authentication is optional. Finally, IPsec supports two modes of operation, that is: Transport Mode, which is used to protect communication between two hosts, and; Tunnel Mode which is used to build virtual tunnels, commonly known as VPNs 10. In the latter mode, both the header and the payload are encrypted and for decryption there is an IPSec-compliant device on the receiving side.

## 2.2 Simulation environment

The simulation scenario of Demand Response Service will be tested and the communication procedure will be analysed. At first, a simplified demand response mechanism will be simulated. The Demand Response platform requests measurements from multiple devices, such as smart meters. The data acquired is used to perform calculations and, according to the results, control signals are sent. Next smarter algorithms will be tested that solve the same technical problem, but are adapted to the constraints posed by the telecommunication infrastructure. The main objective of the simulation is to analyse the effect of the telecommunication infrastructure on the various control algorithms and so to design new algorithms that are able to utilize effectively the underlying telecommunication infrastructure. Thus, networks where: up to hundreds of nodes are organized in a specific topology; point-to-point, unicast and also multicast (or even broadcast) communication, between nodes is being considered, and; traditional layer 3 Internet protocols (TCP/IP) with IPv4 (and probably IPv6) address space are used 11 .

A tree-star network topology can be considered as a combination of two or more star networks connected together. In each of star network comprising the tree, there is a central server to which all the nodes are directly linked. The central computers of the star networks are connected to a main cable called as the "bus". Thus, a tree network is a bus network of star networks. This topology is ideal when the nodes are located in groups, with each group occupying a relatively small physical region. The tree topology structure relies on the main bus cable. In case it fails, the whole network is crippled.

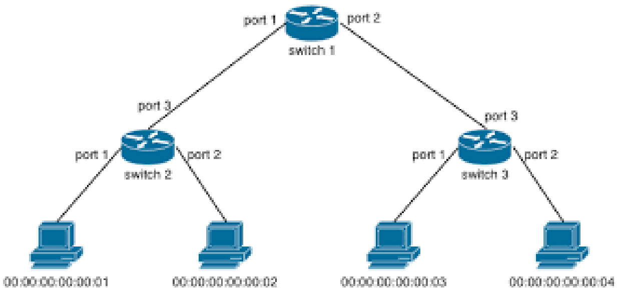

**Fig. 3:** Tree Network Structure

## 3 How 5G can act as "catalyst" in the future smart grid networks

Communication networks for Smart Grids and Smart Meters need to be able to control distributed energy, while simultaneously fulfilling specific performance requirements, as the demand for efficient and reliable communication solutions is expected to grow due to the emergence of smart grids especially in the medium-voltage and low-voltage substations, since these assets currently have no communication or measurement equipment.

The fifth generation of mobile communications -or 5G- actually envisioned as an evolution in mobile communications, can provide economically viable mobile and effective solutions. Verticals like energy are expected to be the new "end-user" thus enabling new applications and/or businesses. In the context of SmarterEMC2, the potential of introducing 5G could be very high, especially in the applications of energy grid control and smart metering; thus, the anticipated performance of 5G will enable communication infrastructure to actively participate in the emerging smart grid and energy scenarios. In order to resolve the new challenges, such as increase of energy demand and storage, smart energy grids will have to focus in data transmission and distributed networks, in the most cost-efficient way.

Due to the development of power plants, new challenges are appearing both for DSO's and telecom operators. Energy production based on solar power plants is more disturbed than traditional power plants, based for example on fossil, while in addition is not stable and varies from day-to-day due to weather conditions (e.g., sun, wind). The need for increased resilience can be met through 5G networks together with increased control, monitoring and protection.

In order to optimize the use of these distributed power plants, a real time dynamic routing of electricity flows is necessary. This routing will require a monitoring and control network, able to transmit distributed data such as measures from smart meters in real time. 5G technology could support efficiently all these services required by the energy sector, providing sufficient flexibility in order to deploy specific virtual network functions and ensure dedicated technical performances with related Service Level Agreements (SLAs) such as latency and Bit-Error Rate (BER).

Smart Grid communication networks consist of multiple domains, each one serving a specific area, for example a distribution network or location such as a secondary substation (where transformation between medium and low voltage takes place). The domain where 5G is expected to play a significant role, is the one of access and backhaul networks, as described in the proposed tree-like topology in the previous Section 2.

Three European Standards Organizations (ESOs), that is CEN (European Committee for Standardization), CENELEC (European Committee for Electrotechnical Standardization) and ETSI (European Telecommunications Standards Institute) have been developing a proper framework to enable energy operators to provide standard enhancement and development in the Smart Grid and Smart Metering fields of the energy market 12, 13.

## 4 Conclusions

The SmarterEMC2 project proposes diverse use cases, some of them requiring ultra-reliability while others requiring low latency communication to smart meters and support of massive number of connected devices. Smart Metering and tree topology as proposed in this paper, demand support of a wireless network that can provide wide area connectivity, optimized for low data rates with high penetration and lower cost at the same time. In this respect, the flexible network architecture proposed by 5G can guarantee reliability, security and performance requirements opening the door to new business roles and responsibilities both on energy and telecom sector.

***Acknowledgments***
The research leading to the actual results has received funding from the European Community's Horizon 2020 Framework Program "SmarterEMC2", under Grant Agreement (GA) No.646470.
The project consortium members are: Intracom S.A. Telecom Solutions (ICOM), University of Durham, Institute of Communication and Computer Systems (ICCS), INESC Porto, Thales Italia S.p.A., Aydem Guneybati Anadolu Enerji Sanayi ve Ticaret Anonim Sirketi (AYDEM), Elektrik Dagitim Hizmetleri Dernegi Baskanligina (ELDER), University of Aalborg (AAU), Hellenic Telecommunications Organization S.A. (OTE) and Fujitsu Laboratories of Europe Ltd. (FLE).

## References

1. X. Fang, S. Misra, G. Xue, D. Yang, IEEE Com. Surv. & Tut. **14**(4), 944-980 (2012)
2. National Institute of Standards and Technology (NIST), *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* (U.S.

Department of Commerce, 2010, November). Available at: https://www.nist.gov/sites/default/files/documents/public_affairs/releases/smartgrid_interoperability_final.pdf

3. CEN-CENELEC-ETSI Smart Grid Coordination Group, *Smart Grid Reference Architecture* (2012, November) Available at: https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf
4. A. Mohd, E. Ortjohann, A. Schmelter, N. Hamsic, and D. Morton, *Proceedings of IEEE ISIE, Cambridge, U.K., June 30 - July 02, 2008, 1627–1632)* (2008)
5. J. Ren, Y. Li, T. Jiang and T. Li, Sec. Com. Netw. **9**(3), 229-240 (2016, February). DOI: 10.1002/sec.539
6. https://www.engineersgarage.com/articles/what-is-zigbee-technology
7. ZigBee Alliance website. Available at: http://www.zigbee.org/
8. S. Kent and R. Atkinson, *RFC 2402: IP Authentication Header* (The Internet Society, 1998, November)
9. S. Kent and R. Atkinson, *RFC 2406: IP Encapsulating Security Payload (ESP)* (The Internet Society, 1998, November)
10. S. Kent and R. Atkinson, *RFC 2401: Security Architecture for the Internet Protocol* (The Internet Society, 1998, November)
11. M. Salehi, J. Proakis, *Digital Communications* (McGraw-Hill Education, 2007, November)
12. CEN-CENELEC Sector, Smart grids found at: https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartGrids/Pages/default.aspx
13. CEN-CENELEC Sector, Smart meters found at: https://www.cencenelec.eu/standards/Sectors/SustainableEnergy/SmartMeters/Pages/default.aspx