A Study of the IoT in the Smart Grid Distribution Networks

Aleksandar Janji[1], Lazar Velimirovi[2], Jelena Velimirovi[2], Zeljko Dzuni[3]
[1] Faculty of Electronic Engineering at University of Niš
14 Aleksandra Medvedeva
Niš 18000, Serbia
{aleksandar.janjic@elfak.ni.ac.rs}

[2] Mathematical Institute of the Serbian Academy of Sciences and Arts
36 Kneza Mihaila, Belgrade 11001, Serbia
{lazar.velimirovic@mi.sanu.ac.rs} {jelena.ranitovic@mi.sanu.ac.rs}

[3] Junis,University of Niš, 2 Univerzitetskitrg
Niš 18000, Serbia
{z.dzunic@ni.ac.rs}

ABSTRACT: *In this work we have studied the Internet of Things and the possible smart grid functions that is supported by IoT. The intelligent real time applications such as real-time monitoring, control and system management are addressed with a smart substation. We found it that these application requires money. However, the Internet of Things have potential in the cost reduction that also help in cyber privacy and security. These issues also pose some challenges and only proper research can help to solve the issues.*

Keywords: Cyber Security, Internet of Things, Smart Grid, Substation Automation

Received: 1 November 2020, Revised 2 March 2021, Accepted 10 March 2021

DOI: 10.6025/ijwa/2021/13/2/45-51

1. Introduction

Smart technologies are significantly influencing the way people live and work today. Objects used daily such as smart phones and smart home appliances are connected to the Internet via intelligent technologies and are able to provide us with large amounts of data on our habits and lifestyles. There are many products and services on energy consumption that citizens may use to make more informed and efficient decisions on problems that matter to them. Technology has already altered our behavior – how we live andwhat we do, for example, the use of social media, mobile apps and open data can help us to reduce energy use.

Nowadays Internet of Things (IoT) applications allow smart energy management and its optimization at all stages: utility operations are improved, power grids are more efficient and resilient, and stakeholders can use these data to allocate resources

IoT empowers consumers (residential, commercial or industrial) by providing control signals and/or financial incentives to adjust their use of demand side resources at strategic times. Energy consumption at the device level can now be tracked through the IoT platforms, and end users can also use these data for processes such as when is the best time to start or shut down a machine, reduce its use at peak hours, waste less energy and, by doing so, reduce their own energy bills.

Concerning the power distribution network, the process of automation and remote control historically started from high voltages and transformer substations of large installed power. The large portion of installed capacities in the medium voltage (MV) and low voltage (LV) distribution network remained without proper monitoring, control, and outside the usual SCADA utility systems. Fast development of information and communication technologies (ICT) lead to the conception of "intelligent transformer substation", and its integration in the smart grid environment.

Considering that smart grid is a large and complex system of interconnected devices that use different protocols for communication between themselves, it is vulnerable to cyber attacks and IT threats. Some security concerns, among others, are customers' security, number of interconnected devices/connectivity and software threats.

2. Smart Distribution Substation

Due to the increasing penetration of dispersed generation, there is a need to increase the intelligence of the components in the MV and LV voltage networks. The increase in sensibility of devices for the quality of voltage and the increasing number of power quality related problems are the reason to look for more functionality in the MV/LV station. The power flows in LV and MV distribution grids will increase their fluctuation as well. To manage these fluctuations while maintaining power quality and reliability, several prototypes of Smart MV/LV substation has been designed [1–5]. These prototypes were focused on particular istribution network problems, like the harmonic voltages, resonance, and peak load reduction.

In general, intelligent components are needed to:

• Get information and influence the power and voltage profile

• Increase the immunity against power quality problems, such as harmonics, voltage dips, flicker

• Reduce the unavailability (minutes of interruption)

• Create micrograds which will be able to work autonomously to increase the reliability as needed

• Enable the usage of condition based maintenance.

A Smart MV/LV substation is built to handle these items. The smart substation concept enables more reliable, more efficient, real-time monitoring and control of the facility nodes installed in the substation. Smart devices can be added to traditional substation devices to perform intelligent functions and provide ubiquitous IT techniques for monitoring, control and management of the system. Similarly to smart homes, each device in the substation is considered as an object and is assigned a unique IP address, transmitting its status and receiving control commands from the utility authorized operator via the Internet.

The main functions of the smart substation are summarized as follows:

• Intelligent analysis for alarm processing, bad data processing, etc.

• Intelligent control for auto-restoration, remedial or predictive action, and emergency state estimation

• Intelligent maintenance and management

• Intelligent physical safety

• Interconnection and application with Geographic Information System (GIS).

The solution presented in [6] relies on an energy management sensors combining monitoring of electrical energy consumption, power quality analysis, and management of electrical energy use in a single powerful internet connected device. With Ethernet or WiFi connectivity and built in web server, sensors can be quickly and easily deployed in any energy management scenario.

Micro RTU Hardware platform is based on ARM platform making the device functional. Micro RTU is designed with two processors: Cortex M4F real time processor with 8 MB of external RAM, serving inputs and outputs in the real time, and Cortex A9 processor with Linux operating system. Its role is to serve the communication interface and data storage.

Central control application performs the periodic polling of remote units in the set of selected transformer substations. Measured values are placed in the RAM of each individual unit. Modbus masters embedded in the central control unit read the Modbus slaves in the remote units, by the TCP protocol through the Virtual Private Network (VPN) formed by the 3G network.

The system requires sophisticated security mechanisms and it is important to note that once performed security evaluation is of a temporary validity only because we face everyday advances regarding the methods for cryptanalysis of cryptographic algorithms. Accordingly, monitoring of security and security re-evaluations of the cryptographic techniques appear as a top-priority issue in the security critical ICT infrastructures.

3. Demand Side Management

The basis of the new smart grid is a trend that reinvents the functioning mode of electric utilities companies - Demand Side Management (DSM). DSM represents the interface between the utility company and smart devices that consume power with the aim of reducing peaks in power grid demand, minimizing power losses in the grid, and increasing the use of unrealized energy savings during low demand periods.

In this way, DSM covers energy efficiency and demand response domains for customers. IoT based management platforms, in other words, deploying energy management measures units at the point of consumption, are a prerequisite for the successful implementation of DSM applications. Electricity customers have at their disposal a variety of options such as rebates, stimulus funds, incentives, with the aim to cash savings for both participants: utilities and their customers. The general architecture of DSM is presented in Figure 1 [7].

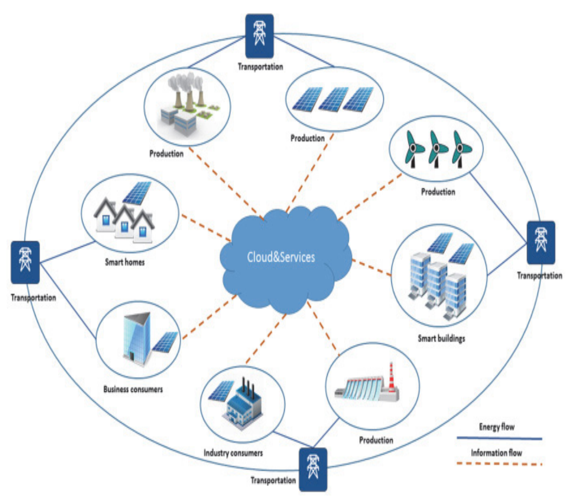

Figure 1. Basic architecture of DSM

Three basic layers can be recognized: a) Cloud and Services – central part of the architecture that collects data from different sources, providing tools and technologies for mass data storage and data processing. b)Utility – this layer collects information from different parts of the power generation supply chains (production, transmission, and distribution) and forwards them to the cloud (data related to the level of current and future production and consumption, the price of electricity, and other information that may affect the DR relation). c) Consumers (smart home, smart buildings, industry) – each consumer represents a node in a complex microgrid. Nodes are equipped with so-called sink or hub that collects information from all smart devices for that node and which has a data storage capacity, local data processing and communication capability to devices outside the node.

Coordination of the huge number of IoT devices which are distributed over the entire platform and acquisition of the necessary data in economically viable manner are some of the major challenges for the implementation of DSM. Taking into account that the DSM applications rely on the IoT architecture, the challenges facing the IoT are also projected on the success of DSM

4. Demand Response

Demand Response (DR) is usually defined as the change in electric usage by end-use customers from their normal consumption patterns in response to changes in the price of electricity over time, or to incentive payments designed to induce lower electricity use at times of high wholesale market prices, or when system reliability is jeopardized. In order to achieve this feature, data about the current consumption of multiple sites during an event should be consolidated in real time through the IoT platform, so the consumer (or the third-party aggregator) can gauge the performance of the entire portfolio almost instantaneously.

The system enables the aggregator to collect customer demand flexibility and provide access to the market. For this purpose, with the development of new features, the aggregator will study which customers can provide profitable DR, actively promote the DR service to customers, and provide financial incentives to the customers to provide DR.

Most DR approaches involve a data concentrator that advises a pool of consumers to reduce their current demand. This approach has repeatedly been shown to be effective for relatively small pool sizes of industrial and commercial consumers. While it remains feasible to signal a small number of consumers and expect an immediate response, DR at a wider areal level is more complex. On these bases, cloud architecture of aggregated consumers is proposed, and the data concentrator with advanced features should be developed.

The possible solution is the platform containing two main subsystems: Energy Hub which is consisted of a power analyzer and appropriate data concentrator, and software enabling the aggregator relationship with both customers and market. The basic architecture of this system is based on Energy Hub and layered-controlled system (Figure 2).

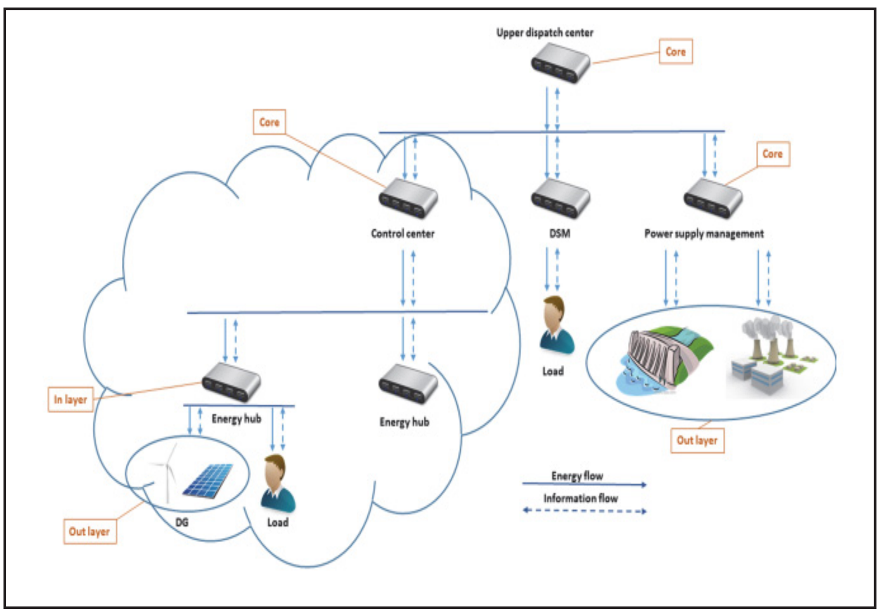

Figure 2. Communication infrastructure

This architecture includes two embedded clouds. A small cloud consisting of the elements which can operate independently is a sub-cloud of the great network cloud. Loads and distributed generation (DG) are controlled by the nearest hub, while the information of loads, power flow, power quality and power market can exchange among each hub and upload to the aggregator dispatch center. The optimal load scheduling plan is made by the aggregator dispatch center. The aggregator dispatch center acting as the cloud core, coordinates the exchange of information, and sends control instruction.

5. IOT Challenges

To build a successful DSM and smart energy concept it is necessary to efficiently cope with several challenges such as energy efficiency, security, privacy and data protection, big data, interoperability, and standardization.

How big and powerful is the IoT network? The IoT refers to a fast-expanding worldwide network of devices connected to the Internet – today there are 4.9 billion connected devices, and it is anticipated that by 2020 there will be 25 billion of them. Moreover, the IoT has the potential to add US$6.2 trillion to the global economy by 2025 [8].

Energy efficiency of IoT devices alone, some of which are expected to be 'always on' and to automatically collect i nformation necessary for users. This feature makes sense only if IoT devices operate on very little power. Otherwise, their application will not have much sense. Although there are significant developments and results in this area that are based on changes in architectural and silicon level, it is clear that achieving the energy efficiency for IoT will not be easy.

Energy efficiency of the devices can be achieved through knowledge extraction from data collected in the early stages. In that way, sending huge amount of data and latency can be avoided. This kind of challenge is better known under the name Edge Fog.Using Machine Learning together with IoT utilities could lead to autonomous grid which is one of the most important challenges in smart grid area.

Another aspect relates to the expected energy efficiency, which is achieved by using DSM-based IoT platforms. Business model that should bring a revolution into energy efficiency domain of smart grid relies on DSM applications and services. It is a crucial change in the concept of energy efficiency, which so far has focused mainly on energy savings in single devices. In this sense, a lot is expected from the IT community, which should contribute with adequate applications, regardless of whether they are great players or startups companies.

Related to the issue of security, there are several topics of interest that need to be considered such as a) generic techniques for cryptographic security evaluation of certain algorithms for encryption, authentication and key management in smart grid application, and b) generic techniques for design of certain cryptographic algorithms for encryption, authentication and key-management.

Security is always a critical issue and challenge for the architects of the system. With the huge number of connected devices, smart grid solutions empowered by IoT are facing security risks both for consumers and for the entire business. The following critical elements of DSM can be identified from the standpoint of security: wireless communication – the possibility of unauthorized access to the devices and collection of sensitive data; cloud-based servers – access and unauthorized use of vast amounts of aggregated data; local network and devices – sending spam, disrupting the normal functioning of devices, shutdown power grid.

Risk of security issues could be reduced by encrypting, using multilayered architecture and other techniques which could be implemented during the product design. Regular software patching for all devices is always welcomed.

Furthermore, IoT devices of the smart grid collect large amounts of personal data relating to consumption and daily consumers habits. Privacy and data protection challenge is directly related to security. By applying the encryption it is possible to protect data privacy. If IoT devices have the possibility of sending anonymized data, it is possible to further reduce the risk of unauthorized access to data.

Data collected from different sources are accumulated in the cloud, which therefore must have a massive data storage and processing capabilities. Big data analytics represents the dominant technique for intelligent processing of data of different structures and formats. The application of the big data concept should always be considered as risky, because there is no simple and unique solution for its implementation. Also, the energy efficiency challenge should be taken into account, since storing the large amounts of data in the cloud also requires power.

The complex architecture of DSM requires communication of an enormous number of devices (M2M – Machine to machine communication). In such an environment, the choice of suitable protocols may directly affect the success of DSM implementation

The complex communication requires adding advanced features which automatically affects the price increase and performance reduction. In the last couple of years, many institutions, such as industry consortia (IEEE, Zigbee Alliance, etc.), standardization bodies, and also some of the leading companies and startups have jointly defined protocols necessary for the advancement of IoT [9].

Their work is mainly focused on adapting IP protocol (6LoWPAN, COAP, and RPL) to enable further expansion of web architecture to the lowest level sensors as well as the development of so-called lightweight protocols, necessary for the interoperability of all devices in the cloud (MQTT, LWM2M, etc.). Nevertheless, interoperability between different vendors, especially those that control different parts of vertical market, remains one of the greatest challenges and roadblocks of further mass deployment of IoT and solutions that are based on it.

Standardization has a key role in removing the technical barriers and ensuring interoperability and reliability. In Europe, standardization of smart metering, as a key component of smart grid, is in the hands of main European Standard Development Organizations (SDOs). Each SDO has responsibility for specific standards: ETSI M2M for interdevice communications, CENELEC (European Committee for Electrotechnical Standardization) for the next generation of electricity meters, and CEN (European Committee for Standardization) for the next generation of non-electricity meters. The following list presents some of general smart metering standards:ETSI TC M2M [10], DLMS/COSEM, MBus ("Meter-Bus"), IEEE 802.15.4, ZigBee and ISA 100.11a, PLC – HEMS, IEEE P1905.1.

Complete list of communication and data exchange standards for smart metering in Europe is available in [11].

Efforts towards smart grid standardization are present worldwide, for example IEEE P2030 [12], ANSI [13], US NIST [14] and IETF [15].

4. Conclusion

The increasing granularity of telemetry in MV and LV networks greatly increases the level of information available to energy intensive industries and utilities. This data must be collected and integrated into existing utility and market operations. This information must also be clearly communicated to customers. There is no doubt that the IoT technology has the potential to be a crucial part of the response of many challenges facing the grid.

More efficient, secure and reliable operation of distribution system can be achieved with the smart substation implementation. The monitoring and control system communicating via Internet with various sensors inside the distribution station and with consumer appliances and sensors is the heart of the Smart MV/LV substation. IT prototype hardware, functions and communication interfaces on an embedded platform based on micro RTU offers the required functionality for the flexible distribution network.

The IoT in power distribution networks is very alike to the problem of auto piloted car: the technology is ready and capable to operate the grid, but even a small anomaly can lead to a disaster. Smart grid architecture and appropriate ICT system have to be carefully designed, in respect of all network stakeholders, and the choice between totally decentralized and centralized system should result in the compromise between them.

Acknowledgement

This work was supported by the Ministry of Education, Science and Technological Development of the Republic of Serbia through Mathematical Institute SASA under Grant III 44006 and Grant III 42006.

References

[1] Hak-Man, K., Jong-Joo, Dong-Joo, K. (2007). A Platform for Smart Substation, *Future Generation Communication and Networking (FGCN 2007), IEEE*, vol 1, 579-582.

[2] Kester, J., et al. (2009). A Smart MV/LV-Station that Improves Power Quality, Reliability and Substation Load Profile, 20th *Intern* Conference and Exhibition on Electricity Distribution - Part 1 *(CIRED 2009)*, Prague, Czech Republic, 8-11 (June).

[3] Heckel, J. (2009). Smart Substation and Feeder Automation for a Smart Distribution Grid, 20^{th} *Intern. Conference and Exhibition on Electricity Distribution - Part 1 (CIRED 2009)*, Prague, Czech Republic, 8-11 (June).

[4] Spack, H., et al. (2010). Intelligent Transformer Substations in Modern Medium Voltage Networks as Part of "Smart Grid", *7th* Mediterranean Conf. and Exhibition on Power Generation, *Transmission, Distribution and Energy Conversion*, Agia Napa, Cyprus, Paper No. MED10/240, 7-10 (November).

[5] Backes, J. (2013). The Riesling Project - Pilot Project for Innovative Hardware and Software Solutions for Smart Grid Requirements, 22^{nd} *International Conference on Electricity Distribution*, Stockholm, Sweden, 10-13 (June).

[6] Janjic, A., et al. (2016). Realization of Smart MV/LV Substation through the Concept of Micro RTU, *10th Mediterranean* Confer. on Power Generation, Transmission, Distribution and *Energy Conversion*, Belgrade, Serbia, 6-9 (November).

[7] Xu Li, D., He, W., Li, S. (2014). Internet of Things in Industries: A Survey, *IEEE Transactions on Industrial Informatics*, 10 (4) 2233-2243

[8] Anyika, J., et al. (2013). *Disruptive Technologies: Advances that will Transform Life, Business, and the Global Economy*, vol. 180, San Francisco, CA: McKinsey Global Institute, 2013.

[9] Francois, J. (2016). Internet of Things in Energy Efficiency: The Internet of Things, *Ubiquity Symposium*, Ubiquity, vol. 2016, (February).

[10] TSI TC M2M, TR 102 691, *Machine-to-Machine Communications* (M2M); Smart Metering Use Cases, 2010.

[11] Fan, Z. et al. (2013). Smart Grid Communications: Overview of Research Challenges, Solutions, and Standardization Activities, *IEEE Communications Surveys & Tutorials*, 15 (1) 21-38, First Quarter.

[12] EEE P2030, http://grouper.ieee.org/groups/scc21/2030/2030 index.html, 2010. [87] ANSI, http://webstore.ansi.org/, 2010.

[13] ANSI, http://webstore.ansi.org/, 2010

[14] Hong, X., Wang, P., Kong, J., Zheng, Q., Liu, J. (2005). Effective Probabilistic Approach Protecting Sensor Traffic, *IEEE MILCOM*.

[15] Baker, F., Meyer, D. (2011). Internet Protocols for the Smart Grid, ETF Internet Draft, (April).