**VSB – Technical University of Ostrava**

Faculty of Electrical Engineering and Computer Science
Department of Electrical Power Engineering

# Proceedings of the 2015 16th International Scientific Conference on **Electric Power Engineering (EPE)**


Supported by
**Central European Energy Institute** CZ.1.07/2.2.00/28.0256

May 20-22, 2015, Hotel Dlouhé Stráně, Kouty nad Desnou, Czech Republic

| | |
|---|---|
| Name: | Proceedings of the 2015 16th International Scientific Conference on Electric Power Engineering (EPE) |
| Publisher: | VSB – Technical University of Ostrava<br>Faculty of Electrical Engineering and Computer Science<br>Department of Electrical Power Engineering |
| Published: | May 20, 2015, Ostrava, Czech Republic |
| Editors: | Stanislav Rusek, Radomír Goňo |
| Edition: | first |
| Circulation: | 300 |
| Cover: | Department of Electrical Power Engineering<br>VSB – Technical University of Ostrava, Ostrava, © 2015 |

The authors are responsible for the contentual and lingual accuracy of their papers and the materials they present.



**Publisher address:**
VSB – Technical University of Ostrava
Department of Electrical Power Engineering
17. listopadu 15
708 33 Ostrava – Poruba
Czech Republic

IEEE Catalog Number CFP1573X - USB

ISBN 978-1-4673-6787-5

# Cyber-physical security for Low-Voltage Smart Grids

## HAN Security within Smart Grids

Robert Czechowski
Department of Electrical Power Engineering
Wroclaw University of Technology
Wroclaw, Poland
robert.czechowski@pwr.edu.pl

***Abstract:*** **Smart Grid is both a concept and a way to mitigate infrastructural Deficiencies and counteract the effects of the growing demand for electrical energy. One of the ways ensuring an increase in power grid's management efficiency is utilization of the latest communication solutions that use of IT technologies. These technologies will help customers and prosumers in the future, in a more efficient management of electricity and the use compatible devices with smart grid technology with the ability to control these devices from a public network (often wireless), users of these devices can meet the same threats as in a typical IT network.**

***Keywords: smart power grid, smart metering, digital security, home area network, security policy.***

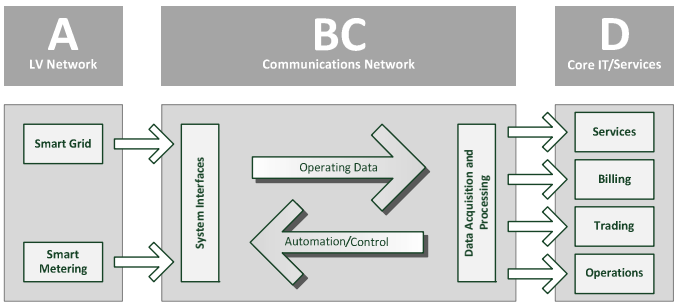
## I. INTRODUCTION

Development of Information and Communication Technologies (ICT) networks cooperating with virtually every industry sector observed in the recent decades met an increased use in comprehensive management in electrical energy transmission and distribution system. This development is headed on increased integration of this grid with a power system where the said grid performs more and more functions integrating the system, i.e. the Supervisory Control And Data Acquisition (SCADA) system supervising the technological process, Power Line Communication (PLC) transmission, or encryption and transmission of control commands. Thereby, utilization of smart solutions, predominantly those within Smart Metering, performs an increasingly important role in ensuring security and reliability of a power system, distribution grids, management of smart devices in home area network included as the (last mile) [1].

The amazing development of information technology and telecommunications creates new tools that can be used in the energy sector, from centralized process management, data mining, to encrypted data transmission by use of PLC and cryptographic algorithms such as Advanced Encryption Standard (AES). Modernization of distribution grids and replacing the traditional electricity meters with smart meters, which is the technical aspect of the modern grid, is not all. A key role that cannot be omitted in such investments is also ensuring electrical security of said grids, which requires familiarity with many issues that are all but unknown to electrical power engineers and security specialists. Implementation of automatic metering devices allows for the structure of a traditional grid to resemble modern ICT grids. Implementation of smart power grids requires cooperation of not only electricians, who will perform the existing installation tasks, but all new specialists in widely understood information technology, starting from network administrators, ICT security specialists, data base and warehouse administrators, up to analysts of layer managing the processes and business layer (Fig. 1).

Infrastructure (AMI) ensures metering possibility of all endpoints and intermediary points in the first and second lines, and automation of communication with them. Intrusions and tampering with such functionality usually have very little effect on the entire power system's performance. One would have a problem with not only tampering with and lowering readings of the meter, but also having to face the risk of depriving many clients of electrical power through mass disconnection of meters' power (switching the relay in the meter) [2].

Increased automation and communication within smart grids certainly comes with many benefits, but it is flawless – due to the availability of the ICT technology in a new, hitherto unknown (for such solutions) branch of industry. There will surely be individuals willing to test their skills and abilities, which will transform into grids' increased vulnerability to attacks. Ensuring years of proper functionality of such grids, their safety and protection from cybercriminals or hackers attack becomes a serious challenges [3].




**Sections:**
A - Infrastructure of Smart Grid Zone - *Smart Grid Communication devices and Smart Meter Network*
B - GSM Technical Management and Communication Zone - *Internet Connections*
C - WAN Zone - *Internet Connections*
D - Infrastructure of Electricity Power Provider Center Zone - *Utility Smart Grid Management Center*

Fig. 1. Basic functionality diagram of the smart Grid and Advanced Metering.

**This paper was realized within NCBR project: ERA-NET,** No 1/SMARTGRIDS/2014, acronym SALVAGE. "Cyber-Physical Security for the Low-Voltage Grids".

978-1-4673-6788-2/15/$31.00 ©2015 IEEE

## II. Threat Classification

Some users are concerned with lack of control over gathering, processing, accessing and using sensitive personal data. The problem, of course, is a little more extensive to this and also concerns unauthorized gathering, acquiring, using and disclosing information obtained by inference from the so-called metadata. That is why it is necessary to implement a comprehensive security strategy for information transfer, personal and telemetry security. Smart Grid and Smart Metering, which simultaneously identify specific devices and their utilization, can disclose clients' profiles and pose new threats to their privacy, such as:

- identity theft,
- disclosure of personal behavioural patterns,
- gathering and grouping consumers by behavioural patterns,
- possibility of disclosure of controlled devices located in a given house or apartment,
- real-time usage monitoring – danger of revealing a consumer's absence in a house or an apartment,
- manipulating energy prices transfer to a meter; e.g. transferring a significantly lowered prices of energy during peak hours and displaying it for many consumers can cause even a significant shift in electrical load. At significant increase in energy consumption by many consumers deceived that way may be dangerous to the grid.

## III. Active Networking Devices in Home Area Network

The main network devices on our home network used to connect to the Internet are routers. Depending on the type of transmission medium (next segment WAN), may have a built-in modem with the appropriate prefix modulation according to the ISP (Internet Service Provider).
Basic friendly features modems used by most Internet service providers are as follows (Fig. 2).

**Modem:** a modem is a device which converts digital signal analog ones and vice versa. Since a telephone line carries only analog signals but a computer works in a digital mode, thus a modem converts analog signals of a telephone line into digital signals. Those can be then read by the computer and also it converts the digital data of a computer into analog signals to be carried by a telephone line. Thus a modem acts as an interface between a computer and a telephone line.

**Router:** a router used in home networks is known as Small Office/Home Office (SOHO) class. It has many features that makes it the perfect solution for our home networks. In addition, if the router during the installation is configured correctly, it can greatly protect your home network from attacks by intruders. An additional advantage in the use of routers is their automatic defence against automated attacks mostly generated by scripts and worms.

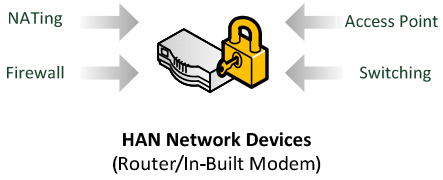



Fig. 2. Functions of HAN edge device.

**Switch:** nowadays provided by the ISP routers, network switches have built-in Ethernet 100Base-TX or 1000BASE-T to connect to different domestic receivers or microcontrollers useful for designing of smart homes. The simplest devices, of this class, have 4 or 8 sockets, so there is no need to purchase separate switch.

**Access Point:** This feature allows you to use a wireless router to connect devices in the IEEE 802.11x (in Europe it is mostly 11abgn). Wireless network coverage allows for easy communication with home automation devices or monitoring.

**Routing:** the technique of transmitting traffic through the router, which involves a change in the source or destination IP addresses. During the routing of altered also the TCP/UDP IP packets. It change, also checksums (both in the IP packet as well as in the segment of TCP/UDP) to confirm the changes. Routing is the technique of transmitting traffic through the router, which involves a change in the source or destination IP addresses. When routing also the TCP/UDP IP packets, and checksums (both in the IP packet as well as in the segment of TCP/UDP).

**NAT:** most systems using NAT, are designed to allow multiple hosts on a private network (devices to network interfaces) to access the Internet using a single public IP address (i.e. the gateway). The two most frequently encountered are translation solutions (Network Address Translation (NAT) and Masquerade (Network/IP masquerading).

## IV. Communication via PLC and GSM in Power Network

The Power Line Communication designates a technology that uses the medium and low voltage electrical networks to provide telecommunication services. Although, since its first applications, when the frequency range started at a low level, PLC is today more commonly used for high-frequency applications (begin known also as broadband power line BPL). The electrical network has been used for a long time by producers and distributors of electrical power for the purpose of network monitoring and remote control at low speed. Nowadays, an electricity producer or distributor cannot ignore standardization. It is worth noting that the deployment of electrical networks, their interconnections, and the constantly increasing number of electrical appliances have resulted in the need of the first network standardization bodies such as the International Electrotechnical Commission (IEC) [4].

The range and speed of data transmission in radio networks can be adversely affected by the presence of other wireless devices and the attenuation of signals by buildings, hills, and even trees. PLC advantage, in this respect, comes from the fact, that these networks do not require a direct line of sight between the transmitter and the receiver, and provide connectivity by

from any location (within a single phase), which are brought power lines. In addition, due to the heavy traffic expected in the Smart Grid networks, especially in emergency situations, they may be overloaded. Therefore, given the nature of the transmitted data redundant communication channel must also be provided (Fig. 5).

**Advantages:** PLC communication considerable interest due to reduction of installation costs relating to the use as a medium for the transmission of the existing electrical system. The strength and popularity of the PLC is also apparent from the considerable efforts of standardization and high availability solutions. HAN systems applications are regarded as the most natural for the PLC. They will also, most likely, be used in Full Smart Grid devices, which will have the ability to configure the host system and the inclusion by the PLC to the ISD (as in the case of DLNA - Digital Living Network Alliance).

**Disadvantages:** technical challenges arise from the nature of power grids. Use of the existing power grid as the transmission medium makes it necessary to take into account the structural deficiencies in the field of high frequency (significant attenuation, impedance change resulting wave reflections and interferences, capacitive and inductive crosstalk) and a significant level of electromagnetic disturbances. Network topology, number and type of devices connected to the network, the distance between the transmitter and the receiver may have a negative impact on the quality of the signal transmitted by a PLC [5].

**The OSI Layered Architecture:** Open Systems Interconnection layered model provides a common base for the description of any data network. This model is composed of seven layers, each describing an independent protocol that provides a service to the layer above it and requests services from the layer below it. In the context of this model, PLC networks correspond to layers 1 (physical) and 2 (data link), supplying an Ethernet connection service to the layers above. Figure 3 illustrates the position of PLC technologies in the OSI model. Layer 1 (physical) is materialized by the electrical wiring that carries the PLC signal. The PLC equipment provides a terminal (typically a PC) with an Ethernet connection service corresponding to layer 2 (data link), using a MAC protocol (Medium Access Control) and RJ-45

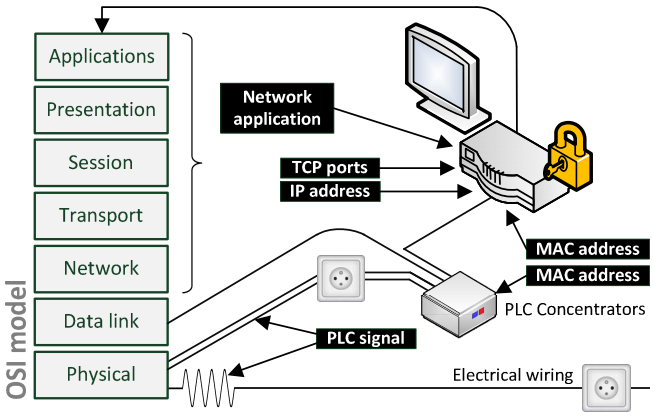



Fig. 3. PLC communication positions in OSI Model.

connectors. The terminal uses PLC network services to access services in higher layers (IP, TCP, HTTP, and so forth). The Physical Layer of PLC technologies is materialized by electrical wiring and, more generally, by electrical networks. In order to transport the PLC signal via this medium, the line frequency (for example 230V/50Hz) of the electrical circuit is supplemented by a modulated signal of low amplitude around a main frequency (carrier frequency).

The Physical Layer consists of this low amplitude modulated signal, transported by electrical wiring at a frequency determined by the PLC technology employed and the applicable regulations.

In addition, the use of open communication standards AMI devices, by their availability, results in greater danger of hackers. The usage of closed and unique communication protocols:

- ensures consistency and uniformity of the system,
- makes difficult hacking attacks,
- limits the scalability of the system,
- increases the cost of the system.

For each data acquisition system for the automatic measurement (AMR, AMI), the key problem is to use the right data transmission technology for a given situation – a suitable transmission medium. When choosing the medium, one should be guided by its reliability, safety, and cost of implementation of the transmission of the whole communication system [6].

## V. HOME AREA NETWORK SECURITY

Safety-related system is referred to a system that ensures the safety of the equipment or facility by the implementation of the safety function, e.g. the function necessary to achieve or maintain a safe state [7].

In order to ensure security in widely understood transmission of electricity, it is necessary to utilize an advanced AMI metering infrastructure which is an integrated collection of elements:

- smart electricity meters,
- communication modules and systems suing the existing electrical grid for transmission,
- concentrators and recorders allowing for bidirectional communication through various media and technologies between the central system and selected meters,
- communication modules and systems interchangeably using the power suppliers transmission medium with another one which directly allows for most commonly wireless connection with the operator's datacentre (Fig. 6).

Security in Smart Grid can be divided into three groups:

a) by the continuity and security of services:

- ensuring continued electrical energy supply at a contractually guaranteed level, binding the supplier and customer (it also concerns cases of bidirectional energy transfer – smart grids with the participation of prosumer),
- ensuring confidentiality of information of clients and security of statistical data generated by them, such as

"consumption amount", time of the greatest energy demand or its total absence,
- security related to energy distribution management process, and telemetry and personal data protection in datacenters,

b) by security class:
- protection from unauthorized access to digital data transmission media and physical security of devices in intermediate stations,
- protection of end-use telemetric devices from unauthorized access, transmission disruption or complete lock of their activities,
- analytical optimization models and decision-making processes,

c) by policy:
- data access policy – user authorization, permission management,
- management security policy – investment processes' principles and rules,
- system security policy – reaction to incidents, managing confidential information like passwords, cryptographic keys.

With knowledge of the ICT network administration, a bit of time and desire in a few steps, we can definitely increase the security of our, own network. The basic functions and also the mechanisms of defence against intruders, can be the following:

**Default Username and Password:** the default username/password set by the manufacturer, allowing access to the configuration router, should be changed and should be set strong enough to prevent unauthorized access to our home. The attacker will firstly attempt to enter its default password for our model, and in turn will make the password he used in other models or similar devices in its class.

**SSID:** the default Service Set Identifier (SSID) is the name of the network and uniquely identifies a particular network and wireless devices must know the SSID of the wireless network to connect to that network. Manufacturers set the default SSID that identifies the device (name betrays their potentially default passwords). SSID is sent in plain text, so it

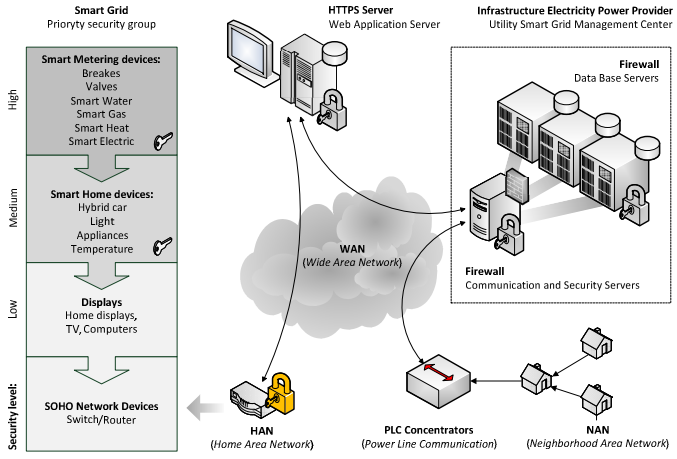



Fig. 4. Paths of information flow in Smart Grid.

can be easily overheard using sniffers, because SSID cannot be treated as protection of network. Some believe that the SSID broadcast should be excluded to impede unauthorized use of the network users. However, this does not improve the security of the network because the SSID is sent by any authorized station when connecting to an access point, and can then be eavesdropped. Not only that, when dispreading off SSID network is vulnerable to masquerading as an access point person with evil intentions, so that the data users of the network may be in danger [8].

**Wireless Security:** there are three types of wireless security on routers or access points:
- WEP (Wired Equivalent Privacy),
- WPA (Wi-Fi Protected Access),
- WPA2 (Wi-Fi Protected Access 2).

It is always advisable to use WPA2 encryption CCMP/AES, which is the safest option if WPA2 is not supported by the router, WPA with TKIP/RC4 is an alternative, but WEP is less secure option and should be avoided because it is as secure as hard to break. WPA may use mode:
- Enterprise – uses a RADIUS server (for business use), which assigns the keys to the right users,
- Personal – does not share the keys to individual users, all connected stations use a shared key PSK (Pre-Shared Key) – it used, e.g. in the HAN or Wi-Fi.

**Limit Network Coverage:** it is always advisable to limit the broadcast coverage of a network to prevent the intruders from gaining access to a home network.

**Disable Remote Management:** this feature should be disabled on the router to prevent intruders from accessing and changing the configuration of the router. If remote administration is necessary, it should be realized via non-standard ports.

**Firmware Update:** one should check to see if there is a new firmware version for the router. After the security configuration in the router, one should make a copy of the settings and store it in a safe place in case of a forced device settings reset.

**Static DHCP reserved IP addresses:** since a router should assign a private IP address to a particular device to share the Internet connection using a DHCP concept, the reserved IP address should be limited, so that a router can't assign an IP address to any device which is trying to get un-authorized access to a home network, the number of IP addresses reserved should be as many as the number of devices in need of internet access within a home network. An additional difficulty is to change from the classic network addressing Class C to Class A or B with a very unique and unusual subnet mask of the initial and final subnet address broadcast address.

**Network Filter:** enabling Media Access Control address filtering in a router whose prevents unauthorized client from getting right IP address and join this network. Devices with addresses that are not included in the filter list addresses, will be dropped, and device which wants to establish a connection cannot access transmission medium. In addition, this

information and the MAC address of the device, along with the date and result of the events will be save in logs of router.

**Universal plug and play (UPnP):** this feature allows network devices to discover and establish communication with each other on the network, this feature makes the initial network configuration easy but it should be disabled when not needed because a malware within a network could use UPnP to open a loop hole in a router firewall to let intruders in.

**Turn-On Firewall:** a router has an inbuilt firewall which should be activated and configured properly to allow authorized users to access a home network, it is advisable to create a black list for unauthorized websites, services etc. Also a firewall should be configured not to reply to ping requests to prevent exposing a home network to intruders, thus firewall should be used to control both incoming and outgoing traffic.

**Network Management Tool:** an efficient network management tool can be used to monitor and manage a network and prevent intruders from having an unauthorized access to a network. Some other security measures are advisable to disable remote upgrade, unnecessary services and Demilitarized Zone (DMZ) features in a router. One should change passwords frequently on all networking devices and make it strong enough, so that it cannot be easily guessed by an intruder [9].

In order to maintain a high level of security, it is necessary to observe predefined procedures and security policies. A grid of meters and concentrators starts to look more and more like a traditional corporate network, which means that similar security measures can be put in place, including systems for intruder detection, access control and event monitoring. Especially vulnerable to packet data attacks are concentrators which, connected to Ethernet switches, utilize the commonly used TCP/IP protocol [1].

## VI. Active Networking Devices in Home Area Network

Communication between the elements of the home area networks should be based on a network with a central gateway (router management). This allows easier (cheaper) implementation of HAN based on proven solutions in computer networks while maintaining high safety standards. The basis of the behaviour of security (including energy), within the HAN, is to provide the network access control by unauthorized persons are not direct participants in the energy management and the media in the context of a particular HAN. Encryption familiar with networks based on 128-bit keys is the recommended solution. Identification of specific devices, in the HAN, requires not only there identified address (eg. IP address), but also determines the type of HAN function parameters and performance characteristics. Communication structure should allow two-way transmission of signals between the elements of the HAN via the home gateway which is the most important part of the communication structure. At the same time, due to public concern about limiting the autonomy of recipients, seems unacceptable to allow direct control (excluding the Local Energy Management System) devices work by external recipients, for example Distribution System Operator (DSO) [10].

**"Smart Grid Ready" Devices:** these are devices which, because of its design and functionality allows adjustment of their power or time to adjust the performance characteristics of on/off without degrading their viability and significant loss of functionality, but do not have a communication interface that is compatible with one of the home area network protocols [11]. These devices are connected to the HAN via intermediate devices:

- converters signals for stand-alone devices or systems, i.e. EIB/BMS, EVSE, RES have different communication protocol or control input,
- Modular Communications Interface (MCI) for devices without communication and control inputs.

**"Full Smart Grid" Devices:** factory-equipped devices in one of the fastest-growing group of communication protocols, i.e. the LAN, Wi-Fi, ZigBee, HomePlug, ZWave, enabling the realization of two-way data encoded with a unique devices address IPv4 and IPv6. These devices must, of course, have the possibility to adjust the performance characteristics in terms of the manufacturer. Set of parameters, that define the characteristics of the work, and the scope of control should be transmitted by the device to the Local Energy Management System through the gates of the home [11].

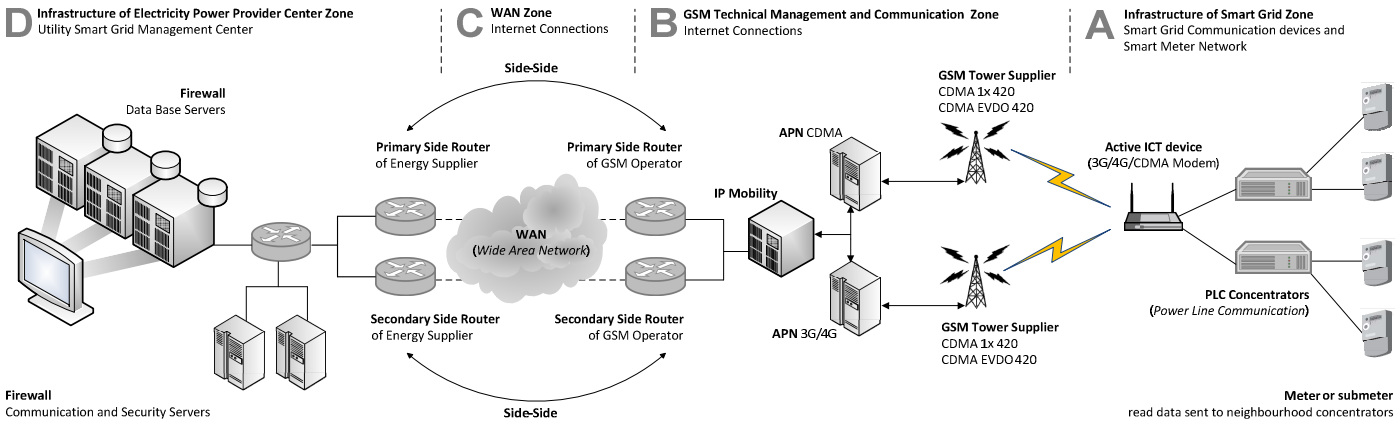



Fig. 5. Smart Grid PLC/GSM infrastructures and communication way.

## V. CONCLUSION

It is quite a challenge to protect each and every one of extensive distribution systems, with cyberterrorism becoming a particularly serious problem. These days, destroying important objects (factories and power plants, but also computer databases) does not require significant power or resources. Examples show that a single person with proper knowledge and access to computer technology is able to perform a successful attack on a power grid. Additionally, cyberterrorism is cheap, it does not put the perpetrator in immediate danger and can be catastrophic in results. By disrupting the operation of banking computer systems, a cyberterrorist could cause a collapse of the world economy. By introducing false data into systems managing a military, power and fuel infrastructure, they could initiate explosions of pipelines, demolition of water intakes and destruction of nuclear power plants [12].

Because of the way of implementation and integration with other existing systems, home area networks for communication between its members should use the medium that not require the ITC infrastructure in the buildings. It is recommended to use electrical installation or one of the wireless signal transmission techniques. It is worth noting that not all home installations or controller of intelligent homes have a physical connection to the electrical system. The HAN combination of wired and wireless home gateway – is part of the responsibility solution for managing the flow of signals – on the model of modern computer networks, management switches and routers. It is desirable, that the power energy consumer or prosumer also to reconfigure the hardware and active by participate in at least a small part of smart grid development. Moreover it is important that the gateway configuration microcontrollers in flat, house or small office are managed by owners.

In the future, an important role in this areas, will be realization of infrastructure and delivering preconfigured devices by Internet Service Provider. With time, we can except more auto-configuration devices. Which at least in part allow simple configurations. Unfortunately, in many cases, this solution will not provide an adequate level of security. There are many methods to ensure safety. Even the very simple solutions such as changing the default password or hiding the name of the wireless network are able to fend off the novice attacker.

On the other hand, we cannot require that each user is a specialist in the range of telecommunications or computer science. Thus, in the next ten years, the electricity supplier will need specialists who possess the practical skills and IT knowledge, which may be used in the energy sector. Smart Grid ICT specialists will take care of not only the home devices configuration or running such systems in Local Area Networks, but also taking care of widely understood security in the information transmission in the Metropolitan Area Network or Wide Area Network. A separate group, will specialise in databases, computer networks, business analysis layers and complex Enterprise Resource Planning systems.

Moreover, it becoming increasingly important to ensure data verification, reliability and security. In order to decrease the amount of incorrect data grids are secured from hackingers attacks. Security policy procedures, that hamper the work of normal application users, are constantly added to. It is not difficult to predict the consequences of such security policies.

**This paper was realized within NCBR project:**
ERA-NET, No 1/SMARTGRIDS/2014, acronym SALVAGE.
"Cyber-Physical Security for the Low-Voltage Grids"

## REFERENCES

[1] T. Flick, J. Morehouse, “Securing the Smart Grid. Next Generation Power Grid Security,” Elsevier Inc. 2011.
[2] K. Billewicz, “Smart Metering. Inteligentny system pomiarowy,” Instytut Energoelektryki Politechnika Wrocławska, Wydawnictwo Naukowe PWN, 2012.
[3] P. Ball. „Masa krytyczna,” Wydawnictwo Insignis, Kraków, 2007.
[4] C. Xavier, „Power Line Communications in Practice,” ArtechHouse 2006.
[5] K. Billewicz, “Problematyka bezpieczeństwa informatycznego w inteligentnych sieciach,” Instytut Energoelektryki Politechnika Wrocławska, 2012.
[6] A.T. Kearney GmbH, „Raport Technologiczny, Infrastruktura Sieci Domowej (ISD) w ramach Inteligentnych Sieci / HAN within Smart Grids”, 2012,
[7] M. J. Cronin, “Smart Products, Smarter Services. Stratiegies for Embedded Control”, Cambrige University Press, 2010,
[8] W. Lewis, “LAN Switching and Wireless: CCNA Exploration Companion Guide (Cisco Networking Academy Program),” Cisco Press 2008.
[9] R.C. Parks, “Advanced Metering Infrastructure – Security Considerations,” Sandia Report, Sandia National Laboratories, November 2007.
[10] R.J. Anderson, “Security Engineering: A guide to building dependable distributed system (Security Policy Model, Monitoring Systems),” 2001,
[11] J. St. John, “A New Standard for the Smart-Grid-Ready Home Appliance,” February 11, 2013, http://www.greentechmedia.com.
[12] A. Fronczak, A. Fronczak, „Świat sieci złożonych. Od fizyki do Internetu,” Wydawnictwo PWN, 2009 r.