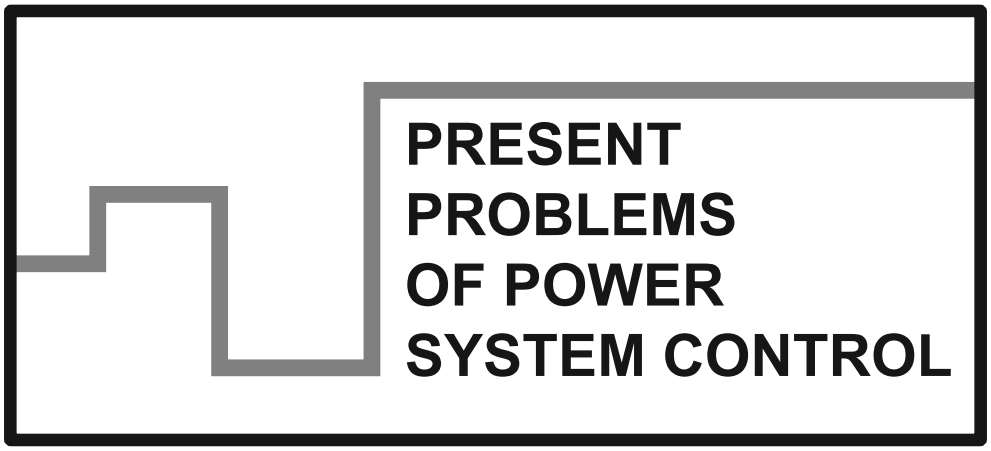
Scientific Papers of
the Department of Electrical Power Engineering of
the Wrocław University of Technology



6

Wrocław 2015

Printed in the camera ready form

Department of Electrical Power Engineering
Wrocław University of Technology
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
phone: +48 71 320 35 41
www: http://www.weny.pwr.edu.pl/instytuty,52.dhtml; http://www.psc.pwr.edu.pl
e-mail: wydz.elektryczny@pwr.edu.pl

OFICYNA WYDAWNICZA POLITECHNIKI WROCŁAWSKIEJ
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław
http://www.oficyna.pwr.edu.pl
e-mail: oficwyd@pwr.edu.pl
zamawianie.ksiazek@pwr.edu.pl

ISSN 2084-2201

Print and binding: beta-druk, www.betadruk.pl

smart power grid, digital security, transport protocol,
smart metering, remote control, security policy

Robert CZECHOWSKI*
Eugeniusz ROSOŁOWSKI*

ITC SYSTEM SECURITY IN THE CONTEXT OF CONTEMPORARY CHALLENGES FOR ELECTRIC POWER INDUSTRY

In recent years, electric power systems, in order to improve their efficiency, are increasingly using the latest innovations in the field of information and communication technologies (ICT) starting from wireless communication and fiber optics systems. Both used for industrial automation purposes and complex data analysis. Those systems, year by year, have made use of more and more sophisticated communication algorithms leading to automatic management of energy distribution process as well as undertaking the system resuscitation tasks as a result of failure. The use of ICT communication equipment in electric power systems is certainly a big advantage, but it also entails some safety issues. The traditional understanding of smart grid cyber security involves the general requirements (placed on existing systems) as well as specific solutions for detection and intrusion prevention (for individual parts of the system infrastructure). Implementation of security policy in management process of the power system, with means of modern technical of digital information transmission, will increase efficiency and reliability of those systems.

1. INTRODUCTION

Electric power systems are currently the highest priority organisms in the hierarchy of state stability assurance. They are referred to as critical systems for a reason. Their proper functioning, entailing production and distribution of electricity, has to be backed by tested management solutions and, more importantly, by utilization of latest technical solutions, not only in terms of business organization concept but also fitting these networks with advanced control and measurement systems. Not so long ago, communication of individual devices installed in a SCADA (*Supervisory Control and Data Acquisition*) central system operator's substations was done entirely based on

* Wrocław University of Technology, Department of Electrical Power Engineering, Wybrzeże Wyspiańskiego 27, 50-370 Wroclaw, Poland, e-mail: robert.czechowski@pwr.edu.pl

serial communication by use of an often specific and dedicated infrastructure. Interestingly enough, the initial expansion stage of these electronically advanced devices included creation of many mutually incompatible standards along with unusual communication interfaces. Producers used the interchangeably, which did not allow for a single leading standard to spread, and, on top of that, they were wrongly convinced that more advanced devices using closed protocols, the basis for their digital communication, would lead to standardization of their technology. An additional problem was often limitations resulting from the protocols themselves, physical interfaces and limited cable length (supplied by the producer) used to connect and run these devices. A few years ago, it was a very common practice to move data from one system to another – usually by use of external storage media. That phenomenon was noticed by companies specializing in production of unusual interface converters that made it possible to transmit signals via a transmission medium convenient to the operator. A definitely better solution which, despite of its simplicity, performed the function of industrial automation remote administration tool was commonplace opening of backdoors in the form of VPN (*Virtual Private Network*) tunnels. Not so long ago, in the scale of digital technology development, a very popular program in industrial automation was Real VNC (*Virtual Network Computing*) [1]. It was widely and recklessly used by novice electrical power system administrators, which led to diminished security level, not only automation and control systems, but also tele-information ones. It was often forgotten (in a rush of emotions associated with the launch of the service) that utilization of virtual tunnels comes with a certain degree of risk. On one hand, we acquire remote control of a distant automation surveillance system, but on the other, that often unsecured system becomes a proverbial gateway for people we would rather not have access our network. Many people forgot to disable the possibility of communication with programs from outside the local network, change the default communication ports or limit communication of the technological process supervising station to a minimum by way of traffic filtering or limiting the number and types of ports allowing for communication with a specific system interface. The above solution was very troublesome, especially for those local businesses and companies whose control and measurement stations were located all over the city (often distanced by several kilometers from each other), an integration of those systems into a single, cohesive one, controlled from one place, was no small challenge.

2. DEVELOPMENT OF TELE-INFORMATION IN ELECTRICAL POWER SYSTEMS

Utilization and popularization of solutions from commonly understood teleinformatics make the development of electrical power systems, in this regard, head in a completely new direction. Their structure already resembles that of modern tele-

information networks – ICT (*Information and Communication Technologies*). Considerable development of information technologies (IT), especially tele-information networks with different scope and area of functionality (LAN, MAN, WLAN and WWAN networks) will allow for fully automatic and remote control of control and measurement systems. Additionally, development of such areas as complex networks will allow control systems for autonomous decision making based on current events and pre-defined rules. A different issue, also being another direction for development of Smart Power Grids (SPG), is not only data analysis but also data mining [2]. Such a process will provide the electric power system operator with completely new information they would not be able to see in a traditional electric power system model. Skillful utilization of this information will allow for not only accurate knowledge and understanding of one's own network's operational logic, but also some real benefits: decreased energy consumption during peak hours, decreased losses due to automated energy balance and increased security of the energy transfer itself. Utilization of IT technologies will contribute to more efficient management of these networks. Unfortunately, their ill-conceived utilization might lead to serious consequences and comes with increased risk of susceptibility to cyber-attacks [3]. Because of variable data transmission media, specific services and complex network architecture, security functions should be considered with multiple layers in mind [4]. It is worth to take note that today's implementation of Smart Grids, because of its specific nature, might attract potential attackers for two reasons. Firstly, it is a critical network fitted with hundreds of devices operating based on the same principles. It allows for multiple reuse of broken security protocols and system vulnerabilities, which makes a potential attack all the more alluring. Secondly, a modern large network can be challenge potential attackers would like to undertake, e.g. to test their abilities. There is a reason IT network administrators are commonly convinced that there is no IT network no one would like to attack. To sum up, utilization of latest tele-information solutions is one of the most effective ways to assure increased effectiveness of electric power systems. It is especially important in heavily urbanized areas with relatively short distances between individual substations.

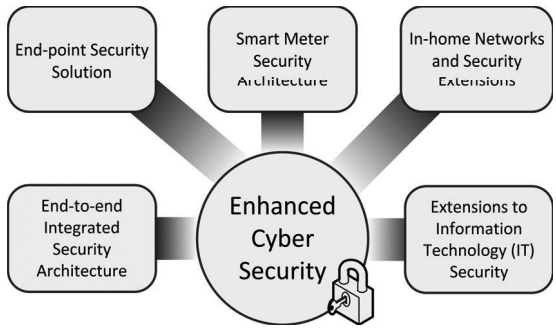


Fig. 1. A conceptual model of a smart grid security system components

Utilization of smart automated devices in networks with dense structures will allow for choosing the best from among available decisions, which can be hard to achieve in suburban and rural systems because of the lack of alternative routes or the need to disconnect large portions of networks. A quite important reason for which such a solution will be viable in the future only in the largest cities is protection of a large group of energy consumers situated within a relatively small area from consequences of a failure, where a long service downtime would entail serious consequences. It does not mean that energy consumers from suburban and rural areas should feel discriminated due to being deprived of such solutions. System distributors have prepared different energy provision solutions for them.

3. TASKS OF SMART AUTOMATION

Rapid development of electric power systems, in the perspective of their utilization in urban agglomerations, makes it so that security automation should be looked at not only in terms of security devices and intended functions, but of whole security systems. It is not always an easy task, especially from the perspective of possessed funding and expected security level. A properly designed security system will allow to react to not only all possible disturbances resulting from the nature of power electric system functionality, but also to intentionally initiated external incidents. Correctly and skillfully configured control and measurement devices can reliably take corrective action. The idea of such a solution is installation, within the network's structure, devices that will automatically communicate with each other and make the best decisions, adequate to a situation at hand. The most important function of smart security automation systems is automatically cutting off a compact line segment and restoring the rest of the system to the normal loss. In short, such devices must possess decision-making logic sufficiently complex to be able to take action in order to mitigate failure consequences in a relatively short time and based on information gathered from the immediate surroundings. Additional function of such a system is transfer and registration of all statistical information and event history to the SCADA operator. One should remember, however, that not even the most advanced logistical programs can ever replace a human, so the highest priority device in the system sends queries to the SCADA system and awaits the system operator's decision.

Electric power security automation can be divided into three groups: elimination automation, prevention automation and restitution automation. The goal of elimination automation is to prevent the spread of a failure's consequences by means of quick and selective elimination of damaged elements of the electric power system. Prevention automation performs an equally important task which is detecting and reporting potential threats and anomalies appearing during normal system operation. A threat might be both overloaded individual system elements and unbalanced active or reac-

tive power in the system. The third kind of automation is restitution automation the task of which is the fastest possible power provision to consumers after a damaged system fragment is shut down. The basic features of security automation are: reliability, selectivity, speed and sensitivity. Such a solution allows for relatively quick restoration of power, and the simple implementation, flexibility and ease of configuration due to decentralized automation allow for fast decision-making with no need for cooperation with SCADA/DMS systems. Smart automation devices can significantly decrease the time to restore power and energy availability in cable distribution networks. In case of a short circuit, they independently isolate one disturbed area and quickly restore power in the network areas unaffected by the short circuit (Fig. 2). The dispatcher is only informed about the short circuit or other system failure, but the automation systems do not await the operator's answer. Instead, they automatically communicate with each other in order to find the short-circuited area, isolate it and restore power in the network areas unaffected by the short circuit.

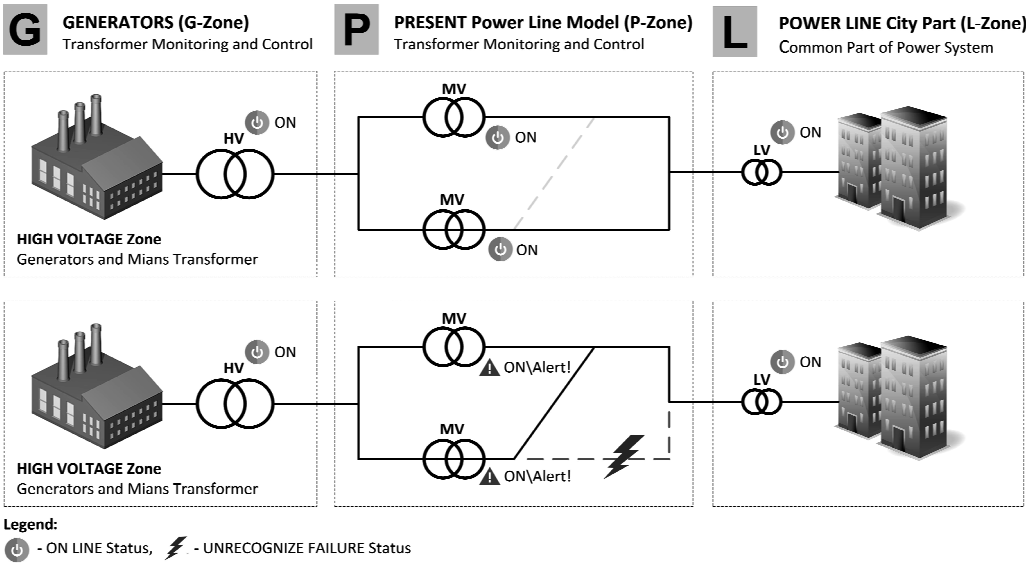


Fig. 2. Exemplary events in the form of short-circuited/damaged electric power lines

Another necessary element of modern electromagnetic systems is a central enterprise resource planning (ERP) system. Such a system, along with SCADA and control and measurement systems, is the basis of modern smart grid systems' functionality [5]. An electric power system's communication system is composed of a transmitter and a receiver, which is interchangeably in the form of security automation devices and communication channels. Utilized media type and network topology provide various levels of communication speed, security, reliability and resilience to external distur-

bances (Fig. 3). There are several types of communication media such as: radio systems, Ethernet, fiber optics, serial connectors or increasingly used communication by means of existing power lines – PLC (*Power Line Communication*). Each of the mentioned media has its own flaws and benefits, their utilization should take into account the potential effect and has to be adequate to specific cases.

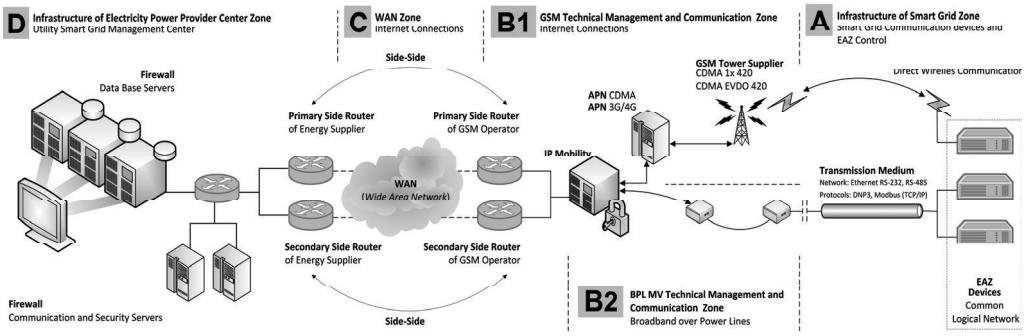


Fig. 3. A conceptual image of security automation communication within a Smart Grid

Communication protocols, being the basis for communication of all tele-information systems, are a collection of rules which allow different manufacturers' devices to communicate with each other. Communication protocols are responsible solely for establishing and controlling network communication, they also set the rules of data representation and are used for error detection and device authentication in tele-information networks. Communication protocols can be divided into two groups. The first one comprises of protocols based on physical protocols, and the second one – with layer protocols. Protocols based on physical protocols have been developed to ensure compatibility between devices offered by different producers, they allow for data transmission at a certain distance (not just locally). The electronics industry association (EIA) has developed universal protocols like RS232, RS422, RS423 and RS485 which are commonly utilized in data transmission. Moreover, these protocols, based on physical ones, are also included in the "physical layer" in the open system interconnection (OSI) model. Communication by means of layer protocols is also accounted for in the OSI model by the International Organization for Standardization (ISO).

All objects in a modern electric power network, from security automation devices to managed switches and routers, operate within a complicated communication structure, most commonly based on the TCP/IP protocol. Such a structure, or more precisely topology, is very varied: from simple serial communication protocols to advanced tele-information networks such as Ethernet networks or WWAN (*Wireless Wide Area Network*). Information exchange, depending on the degree of implementation of a device within the network, is performed on many levels of physical topology,

where each level can make use of different technologies (serial and Ethernet connections – MAN networks, fiber and wireless networks – WAN and WWAN). When talking about the issue of communication, one cannot forget the very important matter of security. Generally speaking, all technical means of detection and prevention of digital threats, ensuring security (of hardware and software), are tasked with protecting the operator's system from unauthorized access to the devices. It concerns all devices, not just at stations, but also in all network segments used by the operator. From the perspective of a potential intrusion, particularly dangerous processes are data transmission, modification or intentional destruction, or DoS (*Denial of Service*) attacks. It is especially important when networks aimed at control of automation devices go outside the physical boundaries of the operator-controlled area. So-called security procedures (security policy) are often omitted in discussions about security.

4. SMART ELECTRICAL POWER SYSTEMS' SECURITY

With the introduction of smart grids, the importance of assuring security for the energy sector grew due to rapid development of IT technologies and telecommunication infrastructures. That is why one should not forget about the security of IT system and information aimed at controlling increasingly varied control and measurement devices. Adequate protection should be considered as early as the design phase. Digital security must cover not only intentional attacks by e.g. disgruntled employees, corporate spies or terrorists, but also accidental endangerment of information infrastructure caused by human errors, equipment failures of natural disasters. Thus, created system vulnerabilities may allow the attacker to gain access into the network and control software and consequently to alter the network's load conditions in order to destabilize it.

Transformation of the current network structure into a smart grid necessitates a number of new security solutions borrowed from already utilized solutions, e.g. from baking systems or public administration. Typical problems of today's IT include hacking, data theft or even cyberterrorism, which will sooner or later also affect electric power grids. Implementation of smart grids by means of installation of remote reading meters, electronic network elements, construction of new IT systems with energy consumption data causes power engineers many entirely new security-related problems. A complex system of multilayered security requires an overall concept of ensuring information security.

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 on 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.

Migration of the current electric power grid model to that of a smart grid entails increasingly more direct investment of IT and telecommunication sectors. These sectors possess already existing cyber security standards that address system vulnerabilities, as well as software aimed at detection of known and potentially dangerous system vulnerabilities. The very same vulnerabilities should be assessed in the context of smart grid infrastructure. Moreover, smart grids will be characterized by additional weaknesses caused by their complexity, large number of shareholders and their operational requirements being time-sensitive.

Traditional understanding of cybersecurity assumes that it's a kind of protection that requires ensuring confidentiality, integrity and availability of an electronic information communication system. When discussing smart electric power grids, the definition of cybersecurity has to be made more extensive. Cybersecurity of smart grids encompasses both technologies and processes of energy systems and cybernetic systems, in operation and management of IT and power systems. These technologies and related processes assure security adequate to maintain confidentiality, integrity and availability of smart grid cybernetic infrastructure, like control systems, security, sensors and actuators.

The general strategy for smart grid security assumes both common requirements and specific ones for individual infrastructure portions. The main task of a cybersecurity strategy should be prevention. Nonetheless, reaction and restoration strategies should also be developed in case of a cybernetic attack on an electric power system.

Implementation of cybersecurity strategy requires definition and utilization of a general smart grid security risk assessment process. Risk is probability of an undesirable incident or event, as well as related consequences. This type of risk is a component of organizational risk. Organizational risk can entail many types of

risk (like investment, budgetary, program management, legal responsibility, security, inventory and information systems-related risks). The process of smart grid risk assessment is based on existing risk assessment means developed by the private and public sectors, and includes identification of consequences, susceptibility to attacks and threats in order to assess the smart grid-related risk. Because Smart Grids entail systems from the IT, telecommunication and energy sectors, the risk assessment process concerns all three sectors and their interaction with smart grids and smart metering.

Generally speaking, the priority goals of IT system security measures include confidentiality, integrity and availability. In industrial control systems, along with power systems, the security priorities are first availability, then integrity and confidentiality. Availability is the most important goal of cybersecurity.

Availability-related time delay in modern Smart Systems can be varied:

- 4 ms for protective relaying,
- sub-seconds for transmission wide-area situational structure monitoring,
- seconds for substation and feeder supervisory control and data acquisition (SCADA),
- minutes for monitoring non-critical equipment and some market pricing information,
- hours for meter reading and longer term market pricing information,
- days/weeks/months for collecting long-term data such as power quality information.

Integrity for power system operations includes assurance that:

- data has not been modified without authorization,
- source of data is authenticated,
- timestamp associated with the data is known and authenticated,
- quality of data is known and authenticated.

Confidentiality is the least critical for power system reliability. However, confidentiality is becoming more important, particularly with the increasing availability of customer information online:

- privacy of customer information,
- electric market information,
- general corporate information, such as payroll, internal strategic planning, etc.

In its broadest sense, cyber security for the power industry covers all issues involving automation and communications that affect the operation of electric power systems and the functioning of the utilities that manage them. This includes the goals of preventing, preparing for, protecting against, mitigating, responding to, and recovering from cyber events. In the power industry, the focus has been on implementing equipment that can improve power system reliability. Until recently, communications and IT equipment were typically seen as supporting power system

reliability. However, increasingly these sectors are becoming more critical to the reliability of the power system. One of the more interesting examples that could help to understand the importance of information transfer efficiency and security for proper electric power system functionality is the system failure from August 14, 2003. Initially small negligence by one of the system operators and the following unfortunate combination of events led to the biggest blackout in the history of the United States. The failure led to a shutdown of 265 power plants (531 power units) in the USA and Canada [6]. Interestingly enough, the on-going and cascading failures were primarily due to problems in providing the right information to the right place within the right time. Also, the IT infrastructure failures were not due to any terrorist or Internet hacker attack; the failures were caused by inadvertent events (mistakes), lack of key alarms, and poor design. Therefore, inadvertent compromises must also be addressed and the focus must be an all-hazards approach.

These hazard most commonly include:

- manmade deliberate threat – incidents that are either enabled or deliberately caused by human beings with malicious intent, e.g., disgruntled employees, hackers, nation-states, organized crime, terrorists, and industrial spies,
- manmade unintentional threat – focuses on incidents that are enabled or caused by human beings without malicious intent, e.g., careless users and operators/administrators that bypass the security controls,
- natural threat – focuses on non-manmade incidents caused by biological, geological, seismic, hydrologic, or meteorological conditions or processes in the natural environment, e.g., earthquakes, floods, fires, and hurricanes.

Providing energy by means of a smart grid includes flow of information allowing for continuous demand monitoring and demand control by means of influencing energy receivers. It will allow for flexible demand shaping and adjustment of supply to the daily demand. In combination with increasingly often utilized energy-efficient building solutions, devices and technological processes, it results in increased energy efficiency on a large scale and reduction of important risk factors – unstable energy balance and low energy efficiency.

Actions to be taken by 2030 for improvement of energy efficiency and development of competitive fuel and energy markets, provided for in the Polish Energy Policy, include particularly:

- implementation of demand side management techniques stimulated by daily variation of electric energy prices resulting from introduction of intraday market and transfer of price signals to receivers by means of electronic meters,
- abolition of limitations related to changing the provider by introduction of nation-wide norms concerning technical prices, installation and reading of electronic energy meters [7].

5. CONCLUSION

An important advantage of a Smart Power Grid is its ability to integrate with an existing energy system in order to intensify development of, among others, distributed generation, connection of renewable energy sources, introduction of energy storage systems and increase energy efficiency, and ultimately realization of the EU climate and energy package's goals [8]. Large-scale introduction of the Smart Grid will initiate changes in the current energy consumption patterns, both for individual (consumers and households) and collective (public utilities) entities. Despite many concerns about grid modernization, better and more directed grid management will contribute to its increased security, which will directly translate into cheaper exploitation and increased service quality.

ACKNOWLEDGMENTS

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] Dokumentacja techniczna Real VNC. Available in: https://www.realvnc.com/products/vnc/
[2] ZAKI M.J., jr., WAGNER M., *Data Mining and Analysis Fundamental Concepts and Algorithms*, Cambridge University Press, 2014.
[3] FLICK T., MOREHOUSE J., *Securing the Smart Grid. Next Generation Power Grid Security*, Elsevier, Inc., 2011.
[4] ANDERSON R.J., *Inżynieria zabezpieczeń. Bezpieczeństwo danych*, Wydawnictwo Naukowo-Techniczne, Warszawa 2005.
[5] Instytut Energetyki Instytut Badawczy, Instytut Energetyki/Badania/Elektroenergetyczna automatyka zabezpieczeniowa, 2012. Available in: https://www.ien.com.pl/consectetur
[6] OZAIST G., *Egipskie ciemności w USA*, Polska Energia, 2012, 5.
[7] Ministerstwo Gospodarki, *Polityka energetyczna Polski do 2030 roku. Załącznik do uchwały nr 202/2009 Rady Ministrów*, Dokument przyjęty przez Radę Ministrów w dniu 10 listopada 2009 r.
[8] Ministerstwo Środowiska, *Pakiet wyzwań – Polska wdraża pakiet klimatyczno-energetyczny. Podsumowanie*, Warszawa 2013.