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

PRESENT PROBLEMS OF POWER SYSTEM CONTROL

5

Wrocław 2014

Cover design

Piotr PIERZ

Printed in the camera ready form

Institute of Electrical Power Engineering
Wrocław University of Technology
Wybrzeże Wyspiańskiego 27, 50-370 Wrocław, Poland
phone: +48 71 320 26 55, fax: +48 71 320 26 56
www: http://www.ie.pwr.wroc.pl/; e-mail: Inst.Energ@pwr.wroc.pl

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

ISSN 2084-2201

Druk i oprawa: EXPOL, P. Rybiński, J. Dąbek, sp.j., ul. Brzeska 4, 87-800 Włocławek
tel. 54 232 37 23, e-mail: sekretariat@expol.home.pl

smart power grid, digital security,
smart metering, security policy

Robert CZECHOWSKI*

SECURITY POLICY FOR LOW-VOLTAGE SMART GRIDS

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 by use of IT technologies. Such solutions ensure reduced energy consumption and evened 24-hour loads, decreased losses and – thanks to automated energy balancing – increased transfer security. Such solutions will directly translate into increased efficiency of the entire power grid. The present article contains an introduction to smart power grids, perspectives for their development in Poland, as well as an extended discussion of related issues concerning security on the organizational level.

1. INTRODUCTION

Development of ICT (*Information and Communication Technologies*) networks cooperating with virtually every industry sector observed in the recent decades has seen an increased use in comprehensive management in electrical energy transmission and distribution system. This development is headed to increased integration of this grid with a power system where the said grid performs more and more functions integrating the system, i.e. the SCADA (*Supervisory Control and Data Acquisition*) system supervising the technological process, PLC (*Power Line Communication*) transmission, or encryption and transmission of control commands by use of open communication standards such as PRIME (standard according to Prime Alliance). 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 and management of smart devices included in the "last mile", the so-called low voltage grid [1].

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

The amazing development of information technology and telecommunications will create 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 AES (*Advanced Encryption Standard*).

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 will requires familiarity with many issues that are all but unknown to electrical power engineers such as security specialists. Implementation of automatic metering devices will allow for the structure of a traditional grid to resemble modern ICT (*Information and Communication Technologies*) grids. Implementation of smart power grids will require cooperation of not only electricians, who will perform the existing installation tasks, but all new specialists in widely understood information technology, from network administrators, ICT security specialists, data base and warehouse administrators, to analytics of the layer managing the processes and business layer.

The new infrastructure constructed according to the new Smart Grid concept will grant the distribution grid operators not only metering or statistical data that can be used by a given supplier to improve the quality of services or increase the income, but also new challenges related to security, which will be evident in the search for specialists and conducting specialized training courses. Integration of power and information systems will, in a couple of years, surely necessitate modernization of curricula at electrical departments in technical universities, including publishing appropriate handbooks. Changes will also include the outlook of hazards each big grid has to face, and security policies which will have to be verified in terms of new design assumptions and potential dangers [2].

If advanced automation of grids and systems is entrusted entirely to external IT companies, it will lead to nobody from the power supplier's side being fully familiar with these often complex power grids and systems, be it electricians or IT technicians. Moreover, there will be a problem of access to the structure and confidential information of the so-called third party (discussed later in this article), which poses an additional threat to the whole system due to dependency on an independent service provider. It is obvious that such a state cannot adversely affect the power infrastructure security and the power sector's subjectivity. The two above issues can be resolved by investing in own personnel through creation of an AMI (*Advanced Metering Infrastructure*) specialized team consisting of electricians and IT technicians or even better – specialists in both these areas.

Basic functionality of the AMI will ensure metering 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) [3].

Next to the completely basic functions of disabling and real-time reading, the AMI has many other functions like control of collection while changing time-zones or displaying prices according to which the automation systems can engage or disengage specific receiver through integration with e.g. the HAN (*Home Area Network*). Tampering with such functions on a large scale may lead to the power system's overload or cause problems to any given consumer by exposing them to costs they would not incur without interference of third parties [2].

One of the main hazards is the possibility of cybercriminals or cyberterrorists' interference, people who seriously impede the continued operation of computer systems and networks, or various electronic systems, depending on the scale of damage [3].

Increased automation and communication within smart grids certainly comes with many benefits, but it is not devoid of flaws, either – 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 translate into these 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 problem [4].

Resources protected in smart power grids are: access to management software, inventory of computer equipment, company's data, personnel (including a list of ICT/AMI specialists), documentation of metering equipment, like e.g. access to the ERP (*Enterprise Resource Planning*) system and company's critical data: data concerning contractors, commercial information, data endangering the positive image, ways of unauthorized access, the so-called Information Security Policy [5].

In summary, attacks on smart power grids can be divided as follows:

a) by the attack location in the power supplier infrastructure:
   - attack on AMI devices (main meters),
   - attack on the data transmission medium, intermediate devices (active and passive),
   - attack on the operator's datacenter (extortion of passwords and access to services by use of various techniques, even bordering on social engineering, attack on access control servers, databases, warehouses and permissions);
b) by the target and scale of a potential attack:
   - attack on a single client [6],
   - attack on the functionality of the entire system or its significant portion [7].

2. DEVELOPMENTAL PERSPECTIVES OF SMART GRIDS IN POLAND

A smart power grid is a solution which proper functioning necessitates implementation of an important mechanism related to energy security, which is management of demand and protection of one's own infrastructure. Supplying energy by use of a smart grid is related to transfer of information allowing for both continued monitoring of demand, and controlling this demand by influencing energy receivers. This will allow for flexible shaping of the demand and adapting the supply to the daily demand. In connection to the increasingly utilized energy-efficient building solutions, devices and technological processes, it leads to a large-scale increased energy efficiency and limiting one of the most serious risks which are: unsustainable energy balance and low energy efficiency.

Thanks to utilization of telecommunication measures, Smart Grid is a way to mitigate infrastructural deficiencies, current imperfections and challenges power grids, in the present form, have to face. Presently, a power grid is characterized by:
– not being able to store energy,
– having to balance production and reception,
– significant technical limitations,
– dependency of the entire economy on the energy supply and prices,
– natural monopoly.

Alteration of this model by increased investments (mainly exchanging meters and modernization of the "last kilometer" with concentrators) will ensure decreased energy usage, balanced daily loads, decreased losses, and translate into significantly increased transfer security. Moreover, the psychological factor of awareness of wasting energy or possibility of using it with decreased costs will make consumers lower their energy demand themselves. It is estimated to be 2–10%.

Table 1. Summary of estimated benefits in Poland until 2020
(* in millions of zloty) [9]

No.	Benefit	Financial dimension of the benefit*	Total*
1	Reading cost reduction	2300	**9480**
2	Savings on unproduced electric energy	2400	
3	Postponed construction of an additional electric power source	1500	
4	Postponing certain investments aimed at increasing a power grid bandwidth	600	
5	Reduction of balance differences including technical and commercial losses	2400	
6	Decreased customer service cost	280	

Estimating the tangible benefits related to reduction of the aforementioned costs to be around 9.48 billion zloty, with implementation costs around 9 billion zloty, it should be recognized that implementation of smart metering systems in Poland is economically viable [9]. The new grid model will not only bring about a revolution in the meter reading system, but also allow for cooperation with previously unusual sources such as photovoltaic panels, wind turbines and hydroelectric power plants. It will be possible to place renewable energy sources in a residential or public building, connected to the grid (after obtaining a license) on the "plug and play" principle, and the smart meters will count separately the amount of energy drawn, and produced and given back to the grid by the micro grid [3].

Provided in the Polish Energy Policy until 2030, actions undertaken to improve the energy efficiency and development of competitive markets for fuels and energy include in particular [10]:

- implementation of Demand Side Management stimulated by daily variation of electric energy prices resulting from introduction of intraday market, and transmission of price signals to consumers by use of electronic meters,
- abolishing barriers concerning a change of supplier through introduction of nationwide standards related to technical features, installation and reading of electronic electricity power meters.

An important feature of a power grid is the ability to adapt it to an existing power system in order to intensify the development of, among others, distributed generation, connecting renewable energy sources, introduction of power storage systems and increase of energy efficiency, consequently realizing the objectives of the EU climate and energy package [11]. Despite numerous concerns related to grid modernization, the better and more directed grid management will contribute to its increased security, which will directly translate into cheaper exploitation. The basic directions followed by the smart grids' development will be:

- increased energy efficiency,
- increased energy security,
- usage development of renewable energy sources, including biofuels,
- development of competitive markets for fuels and energy,
- limited environmental impact of energy.

A few years from now, smart grids will allow for connecting renewable sources, which will result with probability of the entire consumption profile being more predictable and react more quickly to stimuli caused by the active demand management mechanism. The stimulation, in turn, will result from balancing it with currently available power. Development of distributed power's generation sources will contribute to increased energy security of consumers both in the technical (limited risk of power shortage) and economic dimension (limited investments in systemic energetics), but most of all the ecological one (widespread use of renewable energy sources). Introduction of Smart Grid on a larger scale will initiate changes in the existing energy consumption patterns, both in regards to individual entities (consumers and households) and collective ones (public institutions). The consequences of changes introduced in energetics are sometimes compared to changes sparked by the introduction of mobile phones for public use in social telephone communication patterns. The changes in communication system both individual consumers and public institutions. That is why the subject of Smart Grid can and should attract the interest of:

– individual energy receivers (consumers and households),
– entities included in shaping and realization of energy policy and energy planning (energy companies and industry institutions, local government).

There are certain concerns of some consumers related to implementation of smart software. The fear of energy consumption monitoring in flats or houses is so significant that it initiated protests in some countries, like in Holland [12]. However, the very same clients, when purchasing first mobile phones (by which they are under even greater surveillance), not realize the danger related to disclosure and processing of data stored by these phones.

Implementation of Smart Grid will allow for lowering the costs that sooner or later appear during a grid downtime, yet their complete removal is not possible. By use of smart grids, the risk of failure and scale of losses are lowered. That is because the solution allows for demand and supply to be addressed locally, not centrally, which has no negative effect on higher order grids. However, it requires a change of principles in functioning of the market and grid management. From this point of view, construction of smart power grid is essential for development of the economy. Quick development of smart grids will allow for:

– new technologies for electrical and heat energy generation, including renewable energy sources, like small gas turbines, small CHP(*Combined Heat and Power*) plants, fuel cells, wind energy, heat pumps,
– utilization of distributed generation resources (distributed sources, energy storage),
– ICT technologies allowing for developing new methods and systems of grid control, monitoring and security,
– production of end-use energy receivers allowing for integration with Smart end-use Devices,
– new proactive ways of energy market regulation enforcing a change in the present, unfavorable regulation principles of distributed sources,
– change in the way the end-users use energy due to increased awareness (e.g. climate policy, energy security, rising energy costs, energy saving) [8].

In the modernized Smart Grid model, the energy consumer no longer plays just the passive role of power recipient, but consciously and actively manages energy and its usage in their household (building). Grid management by the consumer, and further reshaping it – prosumer, will incorporate conscious saving by use of heating devices (with the greatest power) during the evening hours or outside the peak hours. As the target form, the consumer becomes a prosumer – a micro-scale energy producer. Investment in knowledge about Smart Grid and development of this technology and related solutions should translate into better energy usage and resultant savings (thereby, lower energy bills), as well as into a possibility of income from energy sales – in case of presumption and so-called distributed generation. Even if consumers will not transfer their generated energy surplus to the operator grid, such solution will translate into a decrease of energy drawn from the operator anyway, which will decrease the demand during peak hours. Development of smart power grids requires a conscious and active receiver and consumer of energy, also contributing to the growth of information and low-carbon society, and in the perspective of local government entities – to the growth of energetically sustainable local Smart Communities [3].

The main features of real-time Smart Management:

- bidirectional energy and information transfer,
- decentralized energy generation through micro-stations,
- communication between market entities,
- monitoring of the mains supply,
- monitoring of the peak power,
- monitoring of the infrastructure,
- ongoing energy metering,
- load reduction,
- data registration and visualization,
- gathering data on energy usage by particular receivers,
- sending control signals to devices,
- their remote configuration.

The following definition of a smart power grid is widely accepted: an electrical grid able to harmoniously integrate behavior and actions of all users connected to it: generators, receivers and those who perform both these roles – in order to ensure sustainable, economic and reliable power while retaining a level of security appropriate for the process.

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 datacenter.

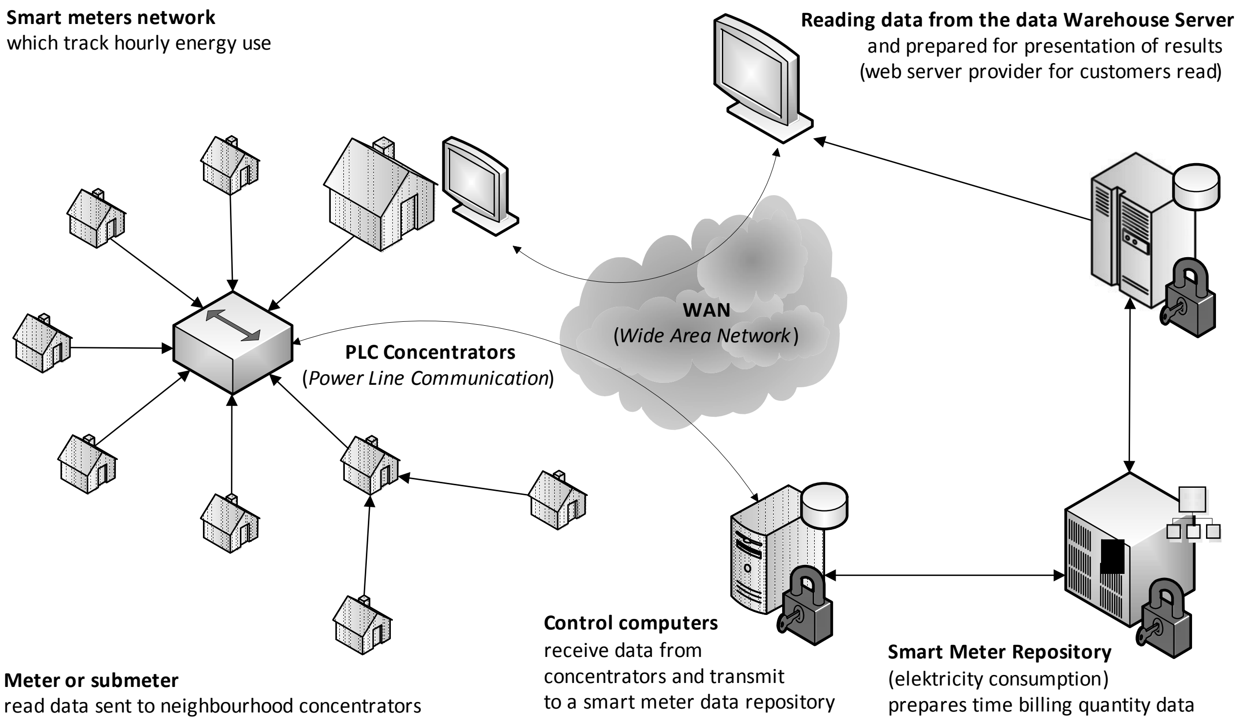

Fig. 1. Paths of information flow in smart grid

One of the main elements of the Smart Grid's functionality is the SM (*Smart Metering*) system – a system allowing for metering, gathering and analysis of energy usage. It consists of energy meters, communication media and software. The system is based on:

- metrology – data gathering and processing,
- telecommunication and computer networks – data transfer,
- computer science and information hardware technology – data processing, storage and presentation.

Intended targets for smart metering:

- creation of a demand management system,
- rationalization of electricity consumption,
- development of a competitive electricity market due to implementation of settlements according to an actual usage profile,
- facilitated switching of suppliers,
- ensuring information on current energy usage in order to allow for energy savings and increased efficiency of its use,
- limited environmental impact of energy,
- introduction of an obligation to use electronic meters allowing for transmission of price signals to energy receivers,
- introduction of nationwide standards related to technical features, installation and reading of electronic electricity power meters [13].

Implementation of a smart grid system presents an opportunity to demonopolize the electric energy market, to regain civil control over the energy sector. However, Smart power grids cannot operate without telecommunication networks.

3. HAZARDS AND SECURITY OF THE SMART GRID

3.1. INTRODUCTION TO SECURITY

The subject of smart grids has long been taking the leading position in programs and publications related to grid development. Smart grids indicate wide application of innovative solutions, from automated electricity meter readings to full utilization of databases' functionality. These solutions will relate to new innovative uses in most of the already existing technologies, in electrical, IT grids and within the energy market. Smart grids are not only a modern infrastructure , but new products and services offered for the benefit of the customer, which will allow for more efficient management of the power grid. The role of the operator is to ensure a modern, energetically efficient and productive infrastructure allowing service and energy providers for unhindered competitive activities in the conditions of growing participation of distributed generation and the active role of energy consumers [14].

Unlike typical acts of mechanical sabotage, an attack on an electronic energy distribution grid can be carried out with little resources, in a coordinated and very precise way. Moreover, it can be initiated via a public network from remote places and performed in the form of a coordinated attack from multiple places at once. Several places can be attacked simultaneously, which can more quickly contribute to discovering weaknesses of the entire security system [1].

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 is starting 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].

Transformation of the current grid structure into a smart grid necessitates a series of novel security solutions borrowed from already used ones. Typical problems of modern computing include hacking, data theft, and even cyberterrorism, which will sooner or later also affect power grids.

Introduction of smart power grids through installation of remote reading meters, electronic grid elements, construction of new information systems consisting of data on energy usage causes energeticists many new security-related problems. A complex multi-layered security system requires an overall concept of providing 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.

Introduction of smart software will contribute to intensified attacks on that grid due to the appearance of a new attack target with a very specific, hitherto unknown architecture which will be a challenge, especially for specialists in computer networks and hosting. ICT systems containing crucial statistical or personal data in one place are particularly exposed to attacks, which will be performed over a computer database on the grid operator's center. If some grid security measures are broken at that time, especially devices responsible for communication and access to concentrators there will not be a possibility to replace them. The learning and dissemination of an effective method to break the security algorithms will not only undermine the entire system, but also entail more expenditures [15]. This happens because there is no technical possibility to easily and cheaply replace these devices software in terms of increased security during access authorization to data and device control. The only possibility of continuous care for a high level of security of these devices is firmware update, and utilization of authentication and encryption based on ID, serial number, password or hash unique to that device and known only to the operator. Based on a given meter's ID, the grid operator can generate a unique code (intended solely for communication with that device only) allowing for further authorization.

Unsecured smart grids implemented today might result in a disaster in the future. A person able to bidirectionally transmit data in metering and billing systems can, to a degree, control pre-payment meters and their internal power disconnection mechanisms. Moreover, they can change the tariff assigned to a meter, and make other changes inconvenient to the consumer and expose them to additional expenses.

Utilization of standard information technologies in power systems is a certain benefit, but it also makes these systems vulnerable to capture. It especially concerns communication standards like PRIME, a fully open, low voltage power line communication standard, available free of charge. The main reasons for arising vulnerabilities in a secured infrastructure are:

- implementation errors,
- closed and poorly tested software,
- errors in system design and security management,
- utilization of obsolete or poorly tested technologies,
- disregard of information security issues.

Utilized solutions have to ensure enough security so even despite a successful attack on one of the grid component, subsequent security breaks do not entail escalating loss of trust in further equipment or services. When designing a secure power grid, one should assume that it will sooner or later be under an attack by a cybercriminal who is familiar with widely used security measures of ICT systems and has enough practical skills to be able to bypass them and properly authorize his or her access to the Smart Grid [1].

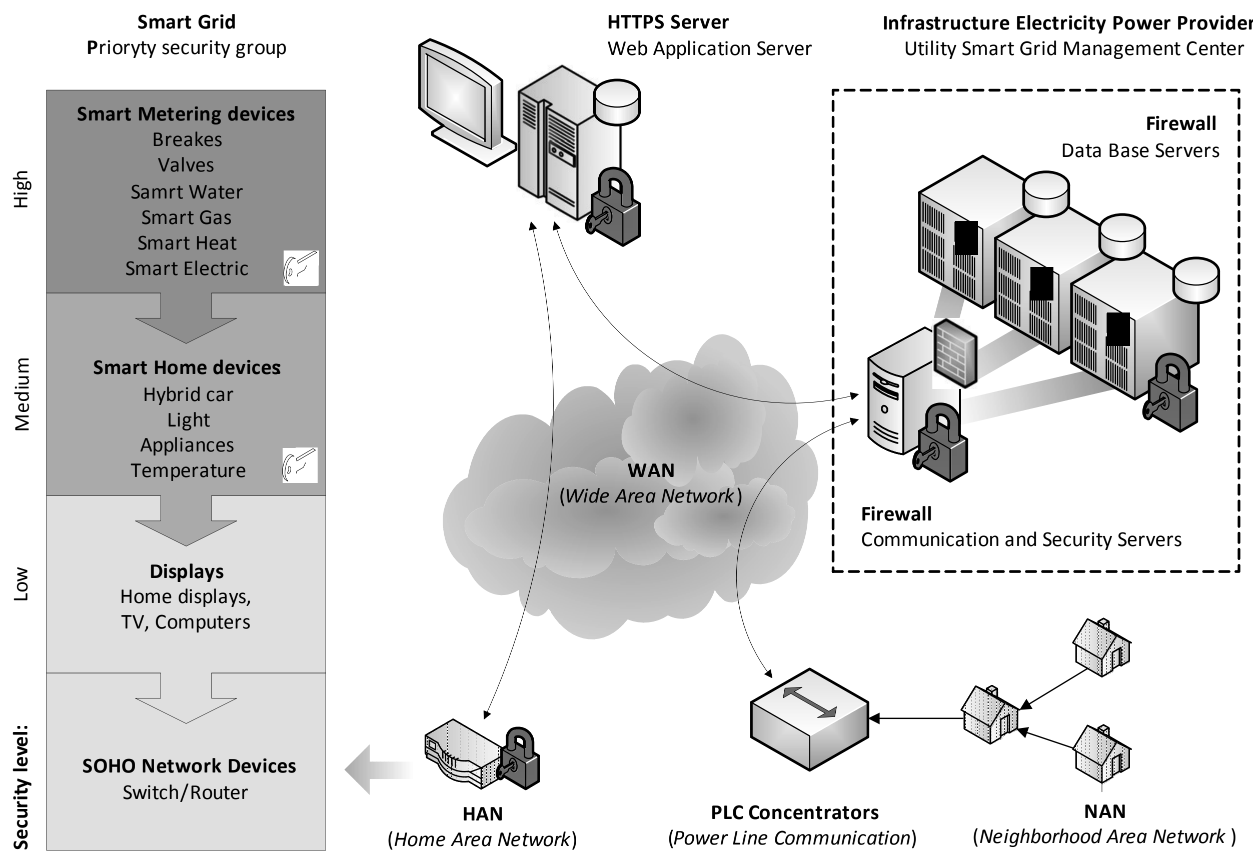

Fig. 2. Smart Grid security model

Such actions may be done via uploading malicious software. That is why proper certifications and advanced authentication methods are required. Unfortunately, these aspects are often disregarded by beginner installers and system administrators, which puts the system at risk of serious consequences already at the initial implementation phase. As indicated by experience from very well secured systems (even the banking ones witch specifics make them considered most secure), not even the best security measures are unbreakable. Using any security means is definitely better than not using one, even if they fail to prevent, they at least significantly impede and limit unauthorized access to the smart grid unauthorized people with average skills and knowledge. It is worth noticing that even average security measures significantly prevent form a successful attack by people who should not have such access at all. It is much more difficult to defend yourself against people with much experience who have previously performed successful attacks of that nature, on grids with similar structure and operating principle. In case of an attack by an "proficient specialist", successful defense depends on multiplicity of mechanisms with various principle of operation, which will ensure enough time for the intrusion prevention or intrusion detection systems to kick in. These systems will be discussed widely in further author works.

3.2. 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 behavioral patterns,
- gathering and grouping consumers by behavioral 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 apartment,
- manipulating energy prices transferred to a meter; e.g. transferring a significantly lowered price of energy during peak hours and displaying it for many consumers can cause even a significant shift in behavior in terms of energy usage, a significant increase in energy consumption by many consumers deceived that way might be dangerous to the grid.

3.3. THREAT SOURCES

The growing energy telecommunication grid is increasingly vulnerable to actions that could disrupt its operation. It is possible to both intercept important information, especially of administrative nature, related to energy commerce, and perform an attack to block the functioning of a given grid portion or service (like access to the database server). What may be particularly dangerous is a potential blockade of real-time information transferring grid functionality related to security and control. Intrusions to the grid can also be performed by authorized users from within the system.

The most common threats to information systems include [2]:

- blocking access to a service,
- hacking into an information system's infrastructure,
- data loss,
- data theft,
- confidential data disclosure,
- information falsification,
- software code theft,
- hardware theft,
- damage to computer systems.

Making an ICT power grid available for the needs of external users is a potential source of threat. It is necessary to separate information transferred for the needs of the power sector to the eternal traffic. Moreover, the administrative and office traffic should also be separated from traffic related to remote supervision over energy facilities. The most commonly encountered problems related to incorrect grid architecture design and its management are:

- lack of proper security architecture,
- errors in information security management,
- software errors,
- human errors and intentional actions,
- insufficient security monitoring.

Lack of clear separation of these grids could potentially cause an intrusion into a power plant control system or a distribution system by way of access through the administrative network, or cause actions blockade and deletion of data from the SCADA system. The causes of such threats are found in:

- vulnerabilities of operating systems which are potential targets for hackers attacks,
- unsatisfied employees, e.g. a fired employee might attempt hacking for revenge or sabotage, incorrectly installing antivirus software and planting malicious software that will cause damage within the smart grid.

4. SECURITY POLICY

4.1. INTRODUCTION TO SECURITY

Systems performing security-related functions consist of such elements as: sensors, programmable devices, communication systems, actuators and power. Abuse related to ICT systems security and failures are becoming increasingly commonplace, possibly resulting in enormous financial losses, lost reputation, high repair costs and even business failure [1].

Smart Grids are of ever more significant strategic value in terms of energy security. A smart grid is a modernization of existing power grids, but it will be subject to the same elementary requirements put forwards for computer networks. In order to ensure basic security, all of the below conditions have to be met:

– confidentiality – ensuring the information is available only to authorized individuals,
– integrity – ensuring accuracy and completeness of information and processing methods,
– availability – ensuring that the authorized individuals have access to information and related assets when it is needed.

In case of violation or failure in meeting the above key norms of AMI systems security infrastructure management, the following rules should be observed:

– each change system configuration requires verification for compliance with security policy,
– failure to observe the system's security policy norms should cause it to be physically disconnected from the grid,
– decision to connect or disconnect the system should me bade by authorized individuals.

Moreover, one should follow a principle of assigning permissions for applications, grid active devices and database systems with regard to permission hierarchy of people managing the entire power system. Access to the resources should only be limited to people allowed to have it. One should also determine:

– the level of acceptable risk,
– access control mechanisms,
– access authorization and identification mechanisms,
– recording changes made within the system: regarding configuration and data modification.

Moreover, it becomes increasingly important to ensure data verification, reliability and security. In order to decrease the amount of incorrect data, grids are secured from attempts to hack and manipulate data hackers should have no access to. 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 a security policy. Security of a system protected this way becomes more and more unattainable. That is why user authorization or access control that differs from statistical passwords becomes the increasingly important [1].

A power system can be considered as one of the most critical systems of strategic importance in functioning of the entire country. Inactivity or destruction of such a system would weaken national security or economic and social wellbeing of the society and its neighbors, both in the physical world and cyberspace.

Protection of the most important infrastructures includes:

– physical security encompassing all predictable threats regarding human errors, systems protection from physical destruction or tampering e.g. with the circuitry, and natural disasters,
– cyber security, a security policy which, apart from the organizational concept of security supervision, includes legal regulations, research work, training courses, etc.

Presently, the functioning of a power grid and efficient control of its operation depend on various computers, computer networks, software and communication technologies, from the point of view of efficient control. While creating one's own security policy, it is a very good practice to place oneself in the role of an attacker. It allows for avoiding the most common mistakes, at the designing stage. Unauthorized interference of a cybercriminal with a computerized power infrastructure may lead to enormous losses resulting both directly (e.g. inability of the enterprise to perform daily operation) and indirectly (e.g. failure to carry out contracts on time, loss of company good image) from power shortage of particular consumers [16].

4.2. SECURITY POLICY MODEL

A critical and often neglected component of this process is a security policy which usually takes the following form: threat model – security policy – security mechanisms.

Security policy is understood as a document which clearly and concisely states the intended tasks of security mechanisms. It results from our understanding of the threats and is a key influence on the construction of our systems. A security policy often takes the form of certain statements regarding which users can have access to which data. It plays the same role in both specifying the requirements of the security system and assessment whether these requirements have been met, similarly to system specification in regards to overall functionality. Indeed, a security policy can be a part of system specification and, just like specification, its main role is to maintain communication.

Security policy model is a concise expression of security properties that are to be present in a system or a generic system type. It is a document in which the entire environment or customer management agrees on security goals. It can also be the basis for a formal mathematical analysis. Security goal is a more detailed description of security mechanisms ensured by specific implementation and their relation to the security goals list. Finally, there is also third the use of the term "security policy" which refers to a list of configuration settings of a security-related product [17].

4.3. MONITORING SYSTEMS

A significant number of secured systems is related to environment monitoring. The most obvious example are electricity consumption meters.

We focus mainly on attacks on communication means (although damaging meters is also somewhat of a concern), but many other monitoring systems are very vulnerable to physical damage. Water, energy and gas consumption meters are usually located within rooms belonging to consumers who may have reasons to cause incorrect meter readings. Such devices are also at a great risk of tampering. In both metering and monitoring systems, we have to provide evidence in order to prove tampering. The opponent could gain the upper hand by not only falsifying communication (e.g. by repeating old messages) but also falsely stating that someone else has done it.

Monitoring systems are also important due to having much in common with systems designed for protection of intellectual property of software and other digital media. They also make for a slight introduction to a wider range of issues related to denial of service attacks, dominating in the industry revolving around electronic threats and beginning to be a serious concern for companies dealing with e-commerce [18].

5. CONCLUSION

5.1. POWER GRID FAILURES

Power grids with transformer stations as nodes and high-voltage lines as edges (in graphical representation) often fall to local failures. Still, in most cases damage resulting in failures of individual stations or transmission lines does not have any significant impact on the functioning of the entire grid. The role of the station (or line) that has been damaged is temporarily taken by a neighboring station (accordingly parallel), and the entire system operates properly. From time to time, however, there are such failures in a power grid where a single failure triggers a cascade of further events and causes transformer stations in large geographical areas to shut down, resulting in enormous financial losses [19].

5.2. CYBERTERRORISM

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 [19].

5.3. DATA SECURITY

From the perspective of data security, The Internet technologies have to abide by the same rules that apply to processing any data. On one hand, generally accepted and still applicable requirements for security-related applications, on the other – requirements regulated by law.

The law of the Republic of Poland encompasses many more or less precise regulations regarding availability, confidentiality and integrity of data process on The Internet. The most numerous ones are confidentiality provisions which not respected results in many sanctions. That is why data security is often limited to confidentiality, protection from unauthorized access. Protected must be encompass content (information, data), possibly other computer system assets which open or close the way to content of shared or otherwise compiled resources. Therefore, practical data security, also in line with provisions of law, includes any and all means and actions undertaken to achieve a predetermined goal [20].

REFERENCES

[1] FLICK T., MOREHOUSE J., *Securing the Smart Grid. Next Generation Power Grid Security*, Elsevier, Inc., 2011.

[2] WILCZYŃSKI A., TYMOREK A., *Rola i cechy systemów informacyjnych w elektroenergetyce*, Rynek Energii, 2 (87), 2010.

[3] BILLEWICZ K., *Samrt metering. Inteligentny system pomiarowy*, Politechnika Wrocławska, Instytut Energoelektryki, Wydawnictwo Naukowe PWN, Warszawa 2012.

[4] BALL P., *Masa krytyczna*, Wydawnictwo Insignis, Kraków 2007.

[5] BILLEWICZ K., *Problematyka bezpieczeństwa informatycznego w inteligentnych sieciach*, Instytut Energoelektryki, Politechnika Wrocławska, Wrocław 2012.

[6] Electronic Privacy information Center, Concerning Privacy and Smart Grid Technology, *The Smart Grid and Privacy*, dostępne w: epic.org/privacy/smartgrid/smartgrid.html, 27.11.2014.

[7] PARKS R.C., *Advanced Metering Infrastructure – Security Considerations*, SANDIA REPORT, Sandia National Laboratories, November 2007.

[8] Urząd Regulacji Energetyki, *Inteligentne sieci – szansa na zwiększenie efektywności energetycznej*, data publikacji: 28.10.2009.

[9] Ministerstwo Gospodarki, Polskie Towarzystwo Przesyłu i Rozdziału Energii Elektrycznej, *Analiza w zakresie ekonomicznej oceny zasadności wprowadzenia inteligentnych form pomiaru zużycia energii elektrycznej w Polsce*, dostępne w: *Bezpieczeństwo gospodarcze/Energetyka/Inteligentne sieci*, 2012.

[10] 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 roku.
[11] Ministerstwo Środowiska, *Pakiet wyzwań – Polska wdraża pakiet klimatyczno-energetyczny – podsumowanie*, Warszawa 2013.
[12] Urząd Regulacji Energetyki, *Inteligentne sieci – Rynek, konsument i zasada zrównoważonego rozwoju*, Warszawa 2012.
[13] Ministerstwo Gospodarki Departament Energetyki, *Perspektywy rozwoju systemu inteligentnego opomiarowania w Polsce*, 28.10.2009.
[14] CZYŻEWSKI R., BABŚ A., MADAJEWSKI K., *Sieci inteligentne – wybrane cele i kierunki działania operatora systemu dystrybucyjnego*, Acta Energetica, nr 1, 2012, 30–35.
[15] A.T. Kearney GmbH, Raport Technologiczny, *Infrastruktura Sieci Domowej (ISD) w ramach Inteligentnych Sieci* (*HAN within Smart Grids*), 2012.
[16] ŻURAKOWSKI Z., *Safety and Security Issues in Electric Power Industry*, 19th International Conference SAFECOMP 2000, Rotterdam, The Netherlands, October 2000.
[17] ANDERSON R.J., *Inżynieria zabezpieczeń (Model polityki bezpieczeństwa)*, Wydawnictwo Naukowo-Techniczne, Warszawa 2005.
[18] ANDERSON R.J., *Inżynieria zabezpieczeń (Systemy monitorujące)*. Wydawnictwo Naukowo-Techniczne, Warszawa 2005,
[19] Fronczak A., Fronczak P., *Świat sieci złożonych*. *Od fizyki do Internetu*, Wydawnictwo Naukowe PWN, Warszawa 2009.
[20] ANDERSON R.J., *Inżynieria zabezpieczeń* (*Bezpieczeństwo danych)*, Wydawnictwo Naukowo-Techniczne, Warszawa 2005.