Michał SZEWCZYK

Silesian University of Technology, Institute of Power Systems and Control

doi:10.15199/48.2015.05.40

Conditions for the improvement and proper functioning of power system automation equipment in the present and the expected future structure of the electric power sector

***Abstract**. An overwhelming majority of equipment and automation systems which are used nowadays are still functioning as autonomous systems and are characterized by the so-called dedicated architecture. This means that for making decisions such devices use mostly signals and information from a local object, regardless of its coexistence with other objects in its most immediate (but also distant) environment. Therefore, the only means of ensuring the object's proper functioning in the present and future conditions is the implementation of hardware structures and algorithms that will have a "territorial" character and will use additional signals and information from other power objects and surroundings. The paper presents conditions for the improvement and proper functioning of power system automation equipment both in the present and the expected future structure of the electric power sector.*

***Streszczenie.** W przeważającej większości współczesne urządzenia automatyki pracują jeszcze jako struktury autonomiczne, charakteryzujące się tzw. architekturą dedykowaną. Oznacza to, że podejmowanie decyzji w takich układach opiera się głównie na lokalnym pozyskiwaniu sygnałów i informacji z najbliższego otoczenia, niezależnie od ich koegzystencji z obiektami sąsiednimi. Dlatego jedynym sposobem na zapewnienie ich właściwego funkcjonowania jest zastosowanie struktur sprzętowych i algorytmów działania o charakterze rozproszonym, pozyskujących informacje z innych obiektów elektroenergetycznych oraz ich otoczenia. W artykule dyskutowane są warunki poprawy i właściwego funkcjonowania urządzeń automatyki elektroenergetycznej w bieżącej i planowanej strukturze systemu elektroenergetycznego. (**Warunki poprawy i właściwego funkcjonowania urządzeń automatyki elektroenergetycznej w bieżącej i planowanej strukturze systemu elektroenergetycznego**).*

Keywords: power system automation, synchronous measurements in the EPS, time synchronization, ICT and IT systems, cybersecurity.
Słowa kluczowe: automatyka elektroenergetyczna, pomiary synchroniczne w elektroenergetyce, synchronizacja czasu, systemy teletransmisyjne i IT w elektroenergetyce, cyberbezpieczeństwo.

Introduction

Today's structures of Electrical Power Systems (EPS) are changing rapidly. This evolution does not only apply to the electricity market. Significant changes are noticeable especially in the power generation philosophy. This is due to many factors. In recent years there has been an intensive effort to introduce new types of power system objects and to increase the participation of renewable sources of electricity in the fuel and energy balance of many countries (e.g. distributed generation sources). This trend entails serious problems with the power system stability, control of operation and protection. There is a growing number of power objects pending implementation or already implemented and working, which can cause serious problems for power automation systems [1-4]. Thus for example, there has been a change in the way of applying the optimal load characteristic of power lines. Where a unidirectional flow of power in the lines was predicted in the design stage, there are bi-directional flows [1-4]. In order to maximize the capacity of load of the transmission lines, the so-called dynamic load capacity and low sag conductors lines have been introduced [1-4]. Wind farms connected to the power grid are characterized by a variable and unpredictable electric power generation. Wind turbines are using power electronics elements and are connected in different locations of the power system. The connection of such electric power sources is dependent on good wind conditions, not the "proper" place from the "point of view" of the power system [1-4]. All of these actions, the complexity and functionality of new power objects, the changing character and ways of operation of these objects, can lead to malfunctioning of different types of power system automation. A vast majority of equipment and automation systems which are used nowadays are still operating as autonomous systems and are characterized by the so-called dedicated architecture. This means that for making decisions such devices use only (or mostly) the signals and information from the local object, regardless of its coexistence with other objects in its most immediate (but also distant) surroundings. The commonly used modes of operation of such equipment are only partially adapted to the new working conditions of the afore-mentioned power objects, as well as the entire EPS. It has been shown that this situation could lead to a number of incidents relating to the EPS [1-4], and consequently even to very large EPS failures (blackouts) [5-6]. The realization of only local protection criteria cannot provide effective protection of power objects from the effects of any disturbances that may occur in them [1-4], [28-29]. Therefore, the only solution to warrant the proper functioning of the EPS is the implementation of hardware structures and algorithms that will have a "territorial" character, will use additional signals and information from other power objects and surroundings, and will be time-synchronized by using high-accuracy time-sources. This in turn results in the need to define and develop the requirements and the physical structure of a data communications network that will enable such functionality. This paper presents an overview of studies, analyses, research activities and it finally stipulates the author's proposed conditions for the improvement and proper functioning of power system automation equipment in both the present and the expected future structure of the electric power sector. Special attention will be paid to the hardware requirements of physical devices, telecommunication systems and software functions provided for the realization of synchronous measurements with reference to the updated IEEE C37.118 Standard and the cybersecurity of ICT systems of the electric power sector.

Basic power system protection principles, hardware structures and their requirements

Power system protection automation has accompanied the EPS for a century. It basic function is to ensure the proper functioning of the EPS and to protect it against the effects of possible failures within the power system. This task is of paramount importance and must be realized as soon as possible. The criteria for the detection and localization of interferences, threats or failures have been worked out for decades. Over the years increasingly stringent requirements for speed, selectivity and reliability have been introduced for power system automation, especially for power system protection devices. At the beginning of the century electromechanical relays were constructed and used. Most of them meet only one simple protection criterion. To satisfy more complicated requirements there was usually a need to link some of the basic devices in a set of protections. Many of the protections of this kind are still used in the EPS. Electromechanical relays are exposed to corrosion, shock vibration, contact bounce and welding. They also require regular maintenance by skilled personnel. This engenders high costs over their lifespan, especially after some first years of life. Hence, they were replaced with solid state electronic devices, which fulfill similar functions using analogue and simple digital/microprocessor devices. These two groups should be clearly differentiated. The first group of devices (simple solid state analogue electronic devices) are very close as regards functionality to electromechanical relays. The second group (microprocessor-based electronic devices) are much more complicated and effective. In many cases they have LCD, keypads and local and remote communication interfaces for changing of parameters and communication with SCADA systems. Protections of this kind are extremely fast, having no moving parts. Accordingly, they are sometimes mistakenly treated as digital devices. What is more, some manufacturers market them as digital devices, which is incorrect. In the "true" digital devices analogue quantities are sampled and converted into digital form for numerical manipulation, analysis, display and recording. This is commonly abbreviated as DSP (Digital Signal Processing). This process provides protection devices with flexibility and reliability which is not attained by any of the other groups of protections. The same basic hardware units can be used for almost any kind of a relaying scheme. Software development and proving procedures are the most expensive items in the whole development, production and life cycle of the overall scheme of digital devices. Digital protections can also be used in self-adaptation schemes, which are impossible in the case of traditional electromechanical or analogue electronic devices. Digital relays are capable of communicating with other devices and hierarchical controllers and systems. The analogue signals coming from CTs and VTs often contain dc offset, harmonics and noise. Thus they are first filtered by means anti-aliasing filters and converted to digital signals by the Analogue to Digital Converter (ADC). Digitized signals are then processed by the measurement and protection algorithms. The accuracy and dynamics of such protections are adequate to the properties of the DSP technique [7-11] and are quite different from the accuracy and dynamics of the solid state electronic protections. Table 1 shows a very simple test of I> criterion for the two types of selected protections: analogue microprocessor-based protection and fully digital protection. It can be seen that the relative error (δ) of pick-up for the analogue device is several times higher than for the fully digital one, and the standard deviation of drop-off/pick-up ratio is almost one order of magnitude lower. That is why the analogue microprocessor-based-only electronic devices cannot be treated on a par with the fully digital protections especially when there are a lot of interfering components in the input signals – currents and voltages from the CTs and VTs – and during the transient states. Usually – disregarding the flexibility, reliability and functionality – "mixing" different types of protections in the closest locations leads to serious problems, concerning mainly the coordination of protection schemes and selectivity. Thus, from the point of view of the hardware structures of power automation devices, the only way to achieve accurate measurements and to ensure the possibility of implementation of complex local and wide-area protection schemes is to use the fully digital units. The best solution is to use the open-structure modular hardware architecture, especially for the wide-area monitoring/protection structures. This type of constructions facilitates fast implementation of new algorithms (firmware upgrade) and makes it easy to change the hardware modules in the devices. Fast communication interfaces should be an obligatory part of devices realized in the form of a convertible module. This approach to hardware requirements will be considered for the wide-area automation structures based on synchronous measurements.

Table 1. Pick-up and drop-off test of I> criterion for two types of selected protection devices using ARTES II testing system *)

I> setting	selected solid state analog electronic microprocesor-based protection device				selected full-digital protection device			
[p.u.]	I_p [p.u.]	I_r [p.u.]	k_{dp} [-]	δ [%]	I_p [p.u.]	I_r [p.u.]	k_{dp} [-]	δ [%]
0.50	0.497	0.476	0.958	-0.600	0.499	0.477	0.956	-0.240
0.75	0.736	0.714	0.970	-1.867	0.751	0.714	0.951	0.107
1.00	0.993	0.967	0.974	-0.700	1.001	0.954	0.952	0.120
1.25	1.244	1.220	0.981	-0.480	1.250	1.192	0.954	-0.032
1.50	1.496	1.461	0.977	-0.267	1.499	1.430	0.954	-0.053
1.75	1.743	1.699	0.975	-0.400	1.750	1.668	0.953	-0.011
2.00	1.981	1.950	0.984	-0.950	2.002	1.905	0.951	0.100
2.25	2.229	2.194	0.984	-0.933	2.252	2.142	0.952	0.071
2.50	2.475	2.463	0.995	-1.000	2.501	2.380	0.952	0.024
Standard deviation of k_{dp}			0.010		Standard deviation of k_{dp}		0.002	

I_r – pick-up value δ – the relative error
I_d – drop-off value k_{dp} – drop-off/pick-up ratio

*) tests for the nominal frequency of input signals without the interfering components

Time synchronization for synchronous measurements in Electric Power Systems with reference to the IEEE C37.118TM2011 Standard

Time synchronization is supposed to co-ordinate at least two processes at the same time, pursued in parallel, independently of their course [17], [19], [25]. This makes it possible to determine which process occurred first in space-time and it helps to establish the chronology of events. The synchrophasor technology requires high-accuracy time-stamping of all the measurements in the power system area [17-25]. There are two main ways to fulfill the above-mentioned requirement. Direct synchronization captures the reference time from the accurate time source for each of the synchronized devices. Indirect synchronization differs from the previous one in that only some parent devices (masters) are synchronized by the accurate time source (e.g. GPS time). The other ones are synchronized (as slaves) with the master devices. In both cases it is necessary to use an appropriate telecommunications network structure and to transfer protocols for accurate flow of time-information between devices [35-38]. The advantage of direct synchronization is the lack of an intermediate stage in the process of synchronization. The big drawback in this case is the need for additional GPS receivers for each of the devices and possible time synchronization errors in the whole analysis area. On the other hand, in indirect synchronization a good knowledge of the transmission network topology can predict the time delay of the signal transmission between devices and it makes it possible to calculate pre-defined time shifts for the synchronizing signal. The application of one of these synchronization methods is dependent on the individual characteristics of the network [36-38], such as the future teletransmission network extension, the number of synchronized devices, visibility of satellites in the area, etc. [20-23], [25]. Synchrophasor measurements shall be synchronized with the UTC time with the accuracy sufficient to meet the accuracy requirements of the Standard C37.118. What merits attention is the fact that a time error of 1 µs corresponds to a phase error of 0.022° for a 60 Hz system and 0.018° for a 50 Hz system. A phase error of 0.01 radian or 0.57° will by itself cause a 1% TVE (*Total Vector Error*) as defined in Equation in [14]. This corresponds to a maximum time error of ± 26 µs for a 60 Hz system, and ± 31 µs for a 50 Hz system. The system must be capable of receiving time from a highly reliable source, such as the Global Positioning System (GPS), which can provide sufficient time accuracy to keep the TVE within the required limits and it is indicative of the loss of synchronization. A special flag in the data output is provided to indicate that a loss of time synchronization shall be asserted when a loss of synchronization could cause the TVE to exceed the limit [13-16], [30].

Based upon several tests carried out in [20], [25] it can be concluded that the cable of specific technical parameters causes permanent offsets of the PPS signal that can be predicted e.g. by knowing the network topology. The cable does not introduce a noticeable random time shift in the transmitted signal. A random time shift can occur e.g. in the wireless network, where it is not possible to achieve constant delays between successive nodes due to the "instability" of the transmission medium and its environment [35-38]. From several studies [20], [25] it can be also concluded that direct synchronization is usually an inferior solution in most cases e.g. due to the synchronization of time based on the data obtained from a different number of visible satellites (especially within the limited areas). A much better solution is an indirectly synchronized system with a specified network layout with one high-level synchronized device. In this configuration, accurate information about the location of each device in the network makes it possible to synchronize all devices with more accurate time-source parameters. Predictably, the introduction of each active switching device (e.g. Westermo T208 switch [20], [25], [47]) into the PPS signal path delays the PPS signal obtained from the GPS receiver. Thus, each additional device or the cable part of the transmission path will trigger a time-delay [25]. However, as it has been previously discussed, some of the delays are fixed. They can be predicted and corrected and therefore they do not affect the quality of time-synchronization. The GPS unit, constructed on the basis of the tested GPS EM-406A device [48], is used e.g. by the Energotest Company to synchronize PMU devices [49]. This unit was also used to conduct functional tests of algorithms allowing the implementation of the forecast PMUs measurements and their functional features. In a PMU network, the Global Positioning System (GPS) is used to provide a precise clock signal. This enables PMUs to give their measurements a reliable time stamp. It should be emphasized that the GPS signal can be jammed [24] and that the PMU network can be mal-operational. This will be discussed later.

Wide-area measurements, synchrophasor techniques and sample physical application

Synchrophasor measurements, i.e. phasor measurements with high-accuracy time stamping, are under consideration for many power system applications such as wide-area monitoring, islanding-prediction and other situational awareness applications [26-29], [31-32]. Synchrophasor measurements are also intended for the power system protection area. Some of the author's research activities have focused on the proper physical realization of synchronous measurements resulting from the Standard requirements [25], [30]. Meeting these requirements can lead to the development of relaying applications that can either be implemented or are considered for future implementation.

The use of high-accuracy measurements and reliable protective algorithms with adequately high accuracy and prompt decision-making qualities [7-12], [26-29] should guarantee an effective operation and protection of the EPS from the consequences of disturbances also in the power system area characterized by a changeable operation frequency over a wide range. The adaptation of measurement and protective algorithms in the cases under consideration has the frequency nature i.e. it concentrates on such a change of the parameters of algorithm operation which guarantees an accurate estimation of measurement and criterion values in a changeable frequency of the input measurement signals – currents and voltages received from the primary circuit [7-12]. The measurement and protective algorithms which are used nowadays in the measurement-protection devices tend to be defined for the constant frequency 50/60 Hz of the input signal, and from the point of view of Standard requirements for synchronous measurements, they are characterized by too big inaccuracies when the frequency of the input signals varies over a wide range [8], [9]. Another problem for the formulation of measurement algorithms is the determination of the level of the insensitivity of these algorithms to the existence of interfering components in the input signals [7-12]. Several interfering components and factors can occur especially in the input measurement signals during faults within the EPS. This situation is accompanied by high penetration levels of intermittent DG (Dispersed Generation) [1-4] and it can significantly affect the EPS. The existence of a thyristor frequency converter is the source of high harmonics, particularly the odd high 5th, 7th, 9th harmonics with the amplitude reaching up to 10% of the amplitude of the basic component [9].

The requirements of PMUs are evaluated by the class of performance. The Standard C37.118.1-2011 defines two classes of performance: the P class and the M class. The P class is intended for applications requiring a fast response and mandates no explicit filtering (protection applications require a fast response). The M class is intended for applications that could be adversely affected by aliased signals and do not require the fastest reporting speed [13], [30]. The letter M is used since analytic measurements often require greater precision but do not require a minimal reporting delay. The user must choose a performance class that matches the requirements of each application. All compliance requirements are specified by the class of performance.

The SmartLoad system is one of sample applications of synchronous measurements based on the C37.118 series of standards. This system [31], [32] is an advanced system designed to make a quasi real-time balance of power and adaptive load-off in the case of a possible active power deficit in the supervised area of a power network. The main advantage of this system, in comparison to the typical Automatic Load Shedding (ALS), is adaptive determination of necessary power shedding and relatively short duration of action (a so called zero-stage of ALS). The standard ALS determines objects which are switched off, and not the real power to be switched off. Taking into account the current load and power import/production (Fig. 1), the system eliminates an unnecessary delay of higher stages (degrees) of ALS. SmartLoad system's operation can be divided into several stages:

- monitoring of the "protected" area
- balancing of power (Fig. 1)
- quasi-real-time determination of potential loads to shed off in case of an active power deficit (basing on quasi real-time synchronized measurements)
- identification of fault
- fast switching-off and balancing of the supervised area (zero-stage of ALS)
- isolation of a balanced island network in case of a continuing frequency drop-off
- further operation as a classic 3-step ALS

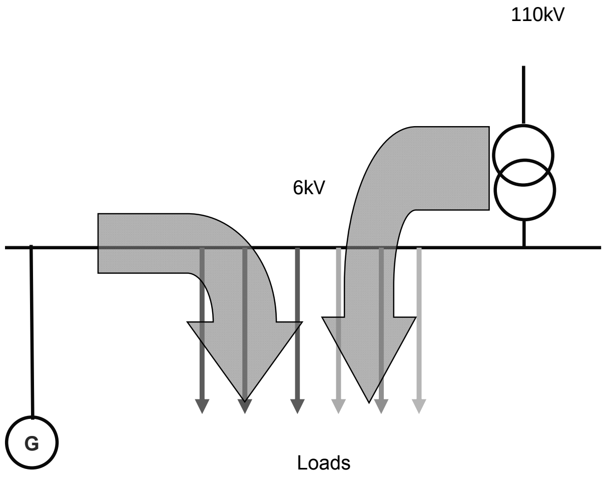

Fig.1 Balancing of power by the SmarLoad system in the industrial application [31]

The system makes it possible to specify locations for which an active power balance is made. A current active power flow is determined for such designated places (usually the ownership boundary). In the case of import of active power to the monitored area, using a multi-criteria algorithm, the system determines a potential load for a shed-off. The current total power "consumed" by loads is almost equal (with a certain margin) to the amount of power "imported" to the area. Thus, in potential isolation from the external power grid (i.e. in the case of a fault), the system "reduces" the power load and creates a quasi-balanced island network area. Therefore, a possible separation from the external power network at the designated point will not cause a significant disruption in the supervised network area. After isolating an island, local generation units adapt themselves to small load changes. The balancing of reactive power within the island can constitute yet another problem. If a reactive power deficit exceeds a predetermined value, a corresponding alarm is generated by a too big reactive power deficit in the case of the creation of an island.

The implemented system has been tested in operational conditions for different industry companies [31], [32]. Figure 2 presents a real fault recording from a sample application of the SmartLoad. Before the failure there was a 8MW import of active power to the analyzed network area. In these conditions, non-intentional island was created beyond the monitored area by the SmartLoad system. In the first phase of this fault the power flow changed to approx. 35 MW of active power "export" to the external power grid area. This resulted in a rapid decrease of frequency on the level of 4 Hz per second. After reaching the frequency of 47.5Hz (setting for switching-off the industrial company from the external power grid) there was "cut-off" from the external network. After 1s the designated loads were "excluded" and a balanced island was created. During the failure the voltage on the busbar dropped from the 6,3kV to below 5,0kV but the network system stayed in operation [31-32].

The first application of the SmartLoad system was based on typical measurement devices. Using synchronous measurements in compliance with the C37.118 Standard caused an even faster and more stable operation of the whole system. This confirms a possible huge potential of the standardized high-precision time-stamped measurement technology.

Teletransmission requirements and the reliability of teleinformatic structures in the EPS

In today's world, the role of IT and ICT systems has dramatically increased. This applies to virtually all areas of our lives [36], including the EPS. Already at the beginning of the last two decades serial connections and modems were used, and even that was available only for a few network locations (especially in the Polish Power Grid). The development of digital and microprocessor technology and IT systems raises the bar for ICT infrastructure of electrical power systems. Systems have started to use fiber-optic cables, and there is also intercommunication between devices which aims at improving conditions for the functioning of protection or surveillance systems and traffic control. IT systems have also been introduced into the administrative part of the power industry and into the customer service. For a long time all these systems operated as isolated local systems. Increasing demands have led to their strong integration. Events in one system affect another system. The same data may be used for different purposes and are available for various parts of IT systems. Because of the topological dispersal of devices within the EPS, there is the need to use wireless communication methods for some applications [35-38]. The complexity of the system is tantamount to an increasing number of vulnerabilities in the ICT network and thus IT energy systems are exposed to the actions of computer hackers or viruses. Adding more users (employees, customers, suppliers) to the network means that the authenticity of the data or users cannot be guaranteed. In addition, the use of ICT network to transmit data unrelated to the needs of power-production, distribution and control/protection systems further increases the need for secure data exchange. Appropriate safety-related equipment and mechanisms are essential to provide the necessary protection of data and information [39], [40]. It is also necessary to separate this information from the data sent to cater for the needs of external users. Cybersecurity in EPS systems and a possible impact of cyberattacks will be discussed later.

In the past, an important role of the security policy was played by the physical network topology and methods of transmission. This has resulted from the massive use of serial links, telephone modems and transmission protocols that are an integral part of the given company-solution. In such cases, there were widely used simple methods of authentication in the form of a paired user-password

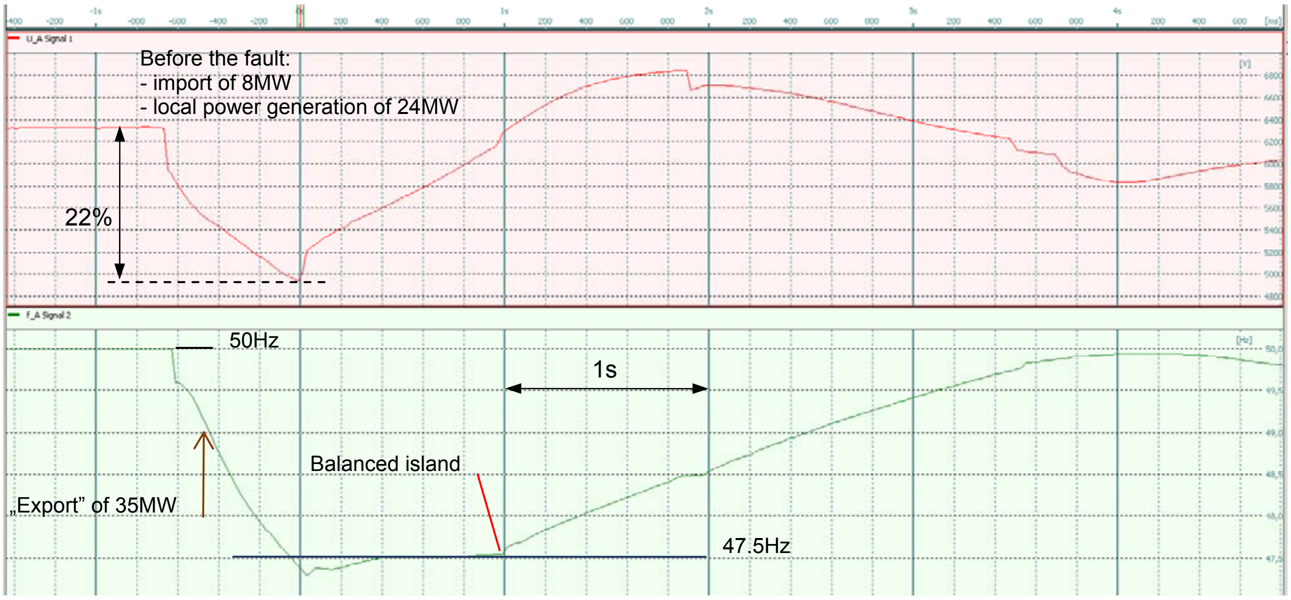

Fig. 2 Real fault recording from a sample application of the SmartLoad system [31]

authentication (most often with the absence of any encryption) [39], [40]. Ethernet-type solutions are now becoming more common in industrial applications, including power generation, transmission and distribution IT infrastructure. This is due to a high flexibility of this solution. TCP/IP communication makes possible to realize reliable data transmission in wide-area networks. Modern network switching devices, applied at all levels of the system, provide the opportunity to build a network fully manageable with predictable quality parameters of transmission. In particular, it is very important for real-time applications.

Shared ICT infrastructure and the use of the Ethernet-based solutions have to change the old approach to the security of systems. The main pillars of safety of today's IT systems by the standards of ISO/IEC 17799 are [38-40]:

- authentication and access control,
- confidentiality of data,
- data integrity,
- non-repudiation.

IT systems are increasingly beginning to move away from the traditional client-server model to virtualization and cloud computing. Hence, the teletransmission network has become a crucial component of the IT infrastructure. A safety analysis promotes the concept of software-defined networking (SDN) [36], [40] in order to comply with all aspects of security, virtualization and mobility. SDN separates the control plane from the data plane. Adaptation of such a model of network guarantees a speedy delivery of services and applications in the IT environment, which in the future will be the basis of automated Smart Grids. SDN latency will be one of the main criteria that determine the success of the implementation of this model. At very high data rates latency cannot exceed the delay of nanoseconds.

Many commonly used data transmission protocols in substation systems were functionally limited. This was due to the specificity of protocol and a well-known tendency of manufacturers to create data transmission systems based on their own solutions. Therefore, automation systems are still experiencing problems relating to the compatibility with individual solutions of different manufactures. In many cases there is a need to use the interface/media/protocol converters and dedicated data concentrators. This affects the performance of such systems, especially in data transmission over long distances. As a consequence of the continuous development of control and protection systems, the problem has been exacerbated. This has resulted in working out a new concept of local and wide-area communication standard (substation and inter-substation communication) – IEC 61850. In guidelines it facilitates achieving full compatibility (at least in principle[*)]) of the solutions proposed by different manufacturers and ensures a preconceived (and predictable) high performance of data transmission and information exchange. From the point of view of the tasks described in the IEC 61850 Ethernet switching devices operate in the second and third layer and must implement features that are essential to ensure an adequate level of data quality. These features are described in IEEE 802.3x, IEEE 802.1p, IEEE 802.1Q and IEEE 802.1w. In the first of these, the main feature is a full-duplex operation mode. This mode does not generate collisions and causes the network to be more deterministic. Another of the standards (802.1p) makes it possible to implement a priority queue. It can be used to change the order of data transmission frames according to the "weight" information. The 802.1Q Standard allows the creation of VLANs. It uses one physical transmission medium to the transparent transfer of data from different networks and greatly reduces the possibility of the so-called collision domains. The last of the afore-mentioned standards, i.e. 802.1w, supports mechanisms for a short recovery time after a failure of connections within the structure of a telecommunications network. Active network switching devices (switches) usually support the creation of logical connections (VLAN) within a specific physical structure of the transmission network. This results in a separation of traffic between several sets of switch's ports, thus increasing the efficiency of switching and transmission within a specific logical network. Communication between virtual networks is possible via a switch working in the third layer. Without additional mechanisms, transmission in such a logical network is invisible to other devices plugged into the switch port which belongs to another VLAN. So using VLAN evades physical limitations of the existing network. It also warrants optimal management of the network structure [38-40].

[*)] there are recorded compatibility problems during physical application [33], [34] The substation LAN is usually built on up to a dozen active switching devices, typically operating in redundant fiber optic rings. High speed data transmission, reliability and redundancy of connections is of paramount importance for systems operating in accordance with IEC 61850. In particular this is most important for GOOSE messages. GOOSE (Generic Object Oriented Substation Events) is a mechanism in which each type of data of various formats (status, value) is divided into sets of data and transmitted in no more than 4 milliseconds. This is the basic mechanism used in IEC 61850 for protection and fast control automation [33], [34].

Cybersecurity of the ICT systems and a possible impact of cyber-attacks on the teleinformatics systems in the electric power sector

With the introduction of Information & Communication Technology (ICT) into the power sector, Electrical Power Systems have become exposed to cyber-attacks and thus have become more vulnerable to them. Smart Grid systems have opened up the power sector to the outsiders and they are more and more dependent on fast global communication and IT systems. Automated operation of grid elements gives many new possibilities but it also leads to several security vulnerabilities. Any cyber-attack on a generation plant can shut the whole plant down. Usually a cyber-attack at one generating-node is unlikely to disrupt multiple plants, but the vulnerability of control systems in a set of plants can cause a serious incident if it is exploited simultaneously in a number of plants. Cyber-attacks within transmission systems are more threatening. In the case of the transmission network most of these attacks may fall into the category of Denials of Service (DOS), Man-in-the-Middle (MITM), packet analysis, malicious code injection or data spoofing attacks. A coordinated attack on automation systems in substations can result in serious damage to the equipment, safety of the operating personnel and disruptions in the integrated operation of the electrical grid. Again, cyber incidents in distribution systems are relatively few because of their low penetration by IT systems. However, distribution systems are becoming more and more centralized. Thus any cyber incident at the central control point can lead to a power supply failure in a large area. From the point of view of the Smart Grid technique, any interruption or the falsification of data collected by the AMI (Advanced Metering Infrastructure) may result in a bad decision taken by other automation systems. AIM use a lot of wireless communication systems. A direct focused beam, which can be modulated from a distance, can cause RF jamming of communication system leading to attacks such as Denial of Service. Attacks threatening PMU networks should also be seriously considered. First and foremost, the loss or jamming of the GPS signal can constitute a serious problem for the reliable functioning of PMUs [24], [25].There are several standards and guidelines that can be used to identify and reduce potential vulnerabilities in the communication networks and ICT systems within the EPS, e.g.:

- IEC TC 57 WG15 Security Standards
- IEC 62351 part 1 to 7
- NERC CIP 002 through 009
- NIST Guide to Industrial Control Systems Security 800-82
- NIST Guide to Smart Grid Cyber Security NISTIR-7628
- Guidelines from Center for Protection of National Infrastructure (CPNI).

Today's cyber-attack activity [40], [50] (Fig. 3) necessitates the adoption of a secure network architecture, especially for control centers. Various network security products like firewalls, IDS/IPS, VPN, IPSec and central logging have to be implemented. Important places and control rooms should be guarded by physical access control devices like biometric scanning, etc. and monitored by CCTV cameras. All applications or proprietary software to be deployed in the Power System applications shall be tested for cyber vulnerabilities. There is also a need to prepare a disaster recovery or a crisis management plan for countering cyber-attacks and cyber-terrorism in the system. Such plans should be continuously tested, updated and the personnel should have adequate training workshops. RTUs and communication equipment should have an uninterrupted power supply with proper battery back-up so that in case of total power failure, supervisory commands & control channels do not fail.

Conclusions

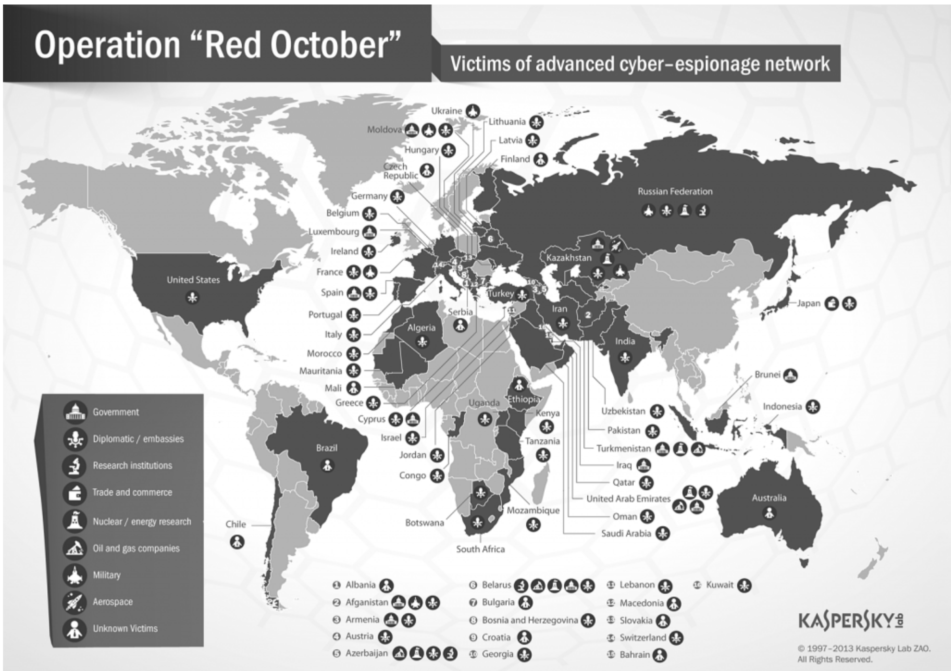

Fig. 3. Victims of the operation "Red October" [50]

The ongoing evolution of Electric Power Systems (EPS), especially distribution systems within the EPS structure, is driven by the implementation of the so-called Smart Grid frameworks. Several research and studies (i.e. [1-4]) have shown that in many cases popular ordinary protective schemes cannot effectively protect power objects from the effects of potential disturbances. New approaches and technologies are required to continue ensuring a reliable and secure energy supply to end users. A fluctuating output from solar photovoltaic and wind plants can cause voltage and power variations in feeders. There are some techniques which can be applied for proper control of operation and protection of the EPS in the present and the expected future structure of the electric power sector. From the point of view of power system automation, first of all there is a pressing need to use fully digital units of known “dynamic characteristics”. Mixing different types of hardware structures will lead to serious problems with the coordination of power system automation. Many of today’s problems as regards the functioning of power system automation result simply from the impossibility of proper coordination of different “operating characteristics” of analogue and fully digital devices. But even in the case of the latter, these characteristics are not the same (different measurement and protection algorithms), which of course necessitates proper standardization and a more profound analysis of power automation algorithms. In particular this applies to the present EPS structure of highly-dynamic behavior. One of the better standardized techniques is the synchrophasor technique. In the Power Grid framework Phasor Measurement Units (PMUs), which adopt a synchronous measurements technique, are recognized to be an invaluable aid in ensuring a secure operation and stability of transmission systems. Time-stamped synchronized measurements could also offer a tremendous benefit to protective relay applications [26-32]. They are real-time measurements which represent current system conditions at any given time and can be used in power system protection schemes. This cannot be done without fast and reliable teletransmission networks [37], [38]. An in-depth analysis of teletransmission structures and proper selection of its devices are important to obtain accurate properties of IT systems. In many cases, such an analysis is restricted only to the basic network parameters such as the necessity “to use fiber optic cables”. Undeniably, this is a basic condition in most cases. However the throughput linked with this transmission medium is not usually the required most important property in EPS teletransmission networks. Much more desirable are the compatibility with the technical solutions of different manufactures, reliability and short permissible delays of transmission (especially for automation purposes). The variation of delay (jitter) is also important for quasi real-time applications. Therefore, the structure of data transmission and the exchange of information of IT systems in the power industry should be designed not only on the basis of fixed guidelines [36-38]. Particular attention should be paid to ensuring adequate security and confidentiality of transmitted data and cybersecurity in general [40]. These features should apply to particular objects and should reflect not just the current needs of the reliability and quality of data transmission, but also a potential implementation of future functionality characterized by much higher requirements. Unfortunately, the standards for teletransmission systems are usually still evolving and they frequently cannot keep up with the dynamic changes in the functionality and the specificity of the ICT systems in EPSs. Every possible EPS point of contact with public telecommunication networks is a potential point of an attack on this type of network. The experiences of recent years have indicated that for this type of networks security issues are not handled carefully enough. There have been many attacks on theoretically well-protected networks of banks and large corporations (including government sites – Fig. 3). An attack which takes advantage of some vulnerability (i.e. CVE-2014-0160 - the so-called Heartbleed) can result in not only obtaining a private key of websites or secured terminals, but it also makes it possible to gain access to user passwords and confidential information due to the possibility of easy decryption of secure data. Therefore, new functionalities should be introduced into the communication systems in the EPS very cautiously indeed and they should undergo rigorous safety tests.

Most local automation algorithms cannot meet all the requirements of the today’s EPS. This occurs especially when there is no communication with other devices/systems or when a teletransmission system is malfunctioning. It should be emphasized that wide-area measurements and algorithms seem to be the only way to real improvement of the functioning of automation systems. Nevertheless, due to a possible loss of communication, local-only algorithms should be still developed, especially those which are based on artificial intelligence techniques [41-46].

REFERENCES

[1] A. Halinka, P. Rzepka, M. Szablicki, M. Szewczyk: Wpływ możliwości podejmowania błędnych decyzji przez zabezpieczenia odległościowe linii dystrybucyjnych WN z przyłączonymi odczepowo farmami wiatrowymi na bezpieczeństwo pracy SEE, „Rynek Energii nr I (V), maj 2010”, pp. 156 – 161

[2] A. Halinka, P. Rzepka, M. Szablicki, M. Szewczyk: Wpływ poprawności pracy automatyki elektroenergetycznej na bezpieczeństwo SEE w aspekcie nowych rozwiązań technicznych i ekonomicznych realizowanych i planowanych do realizacji w KSE, Przegląd Elektrotechniczny, R. 87 NR 2/2011, pp. 140 – 143

[3] A. Halinka, P. Rzepka, M. Szewczyk, M. Szablicki: Przyłączanie farm wiatrowych - potrzeba nowego podejścia do sposobu funkcjonowania automatyki elektroenergetycznej sieci WN, Przegląd Elektrotechniczny, R. 87 NR 9a/2011, pp. 218-221

[4] A. Halinka, M. Szewczyk: Distance Protections in the Power System Lines with Connected Wind Farms, Chapter in the book „From Turbine to Wind Farms - Technical Requirements and Spin-Off Products”, Edited by Gesche Krause, InTech, April 2011, 218 pages

[5] AWARIA SYSTEMOWA W DNIU 4 LISTOPADA 2006 – raport końcowy opracowany przez Komisję Poawaryjną w oparciu o dostępne informacje dotyczące awarii systemowej w dniu 4 listopada 2006 roku i opublikowany przez UCTE

[6] Raport Zespołu ds. Zbadania Przyczyn i Skutków Katastrofy Energetycznej powołanego zarządzeniem Wojewody Zachodniopomorskiego nr 154/2008 z dnia 22 kwietnia 2008 roku

[7] „Badanie dokładności metrologicznej toru pomiarowego układu decyzyjnego zabezpieczeń elektroenergetycznych w szerokim zakresie zmian częstotliwości", Raport końcowy Projektu Badawczego KBN: N505 024 31/3647, kierownik projektu: dr inż. Michał Szewczyk

[8] W. Rebizant, J. Szafran, A. Wiszniewski: Digital Signal Processing in Power System Protection and Control, Springer London Ltd, 2013

[9] A. Halinka, P. Sowa, M. Szewczyk : Measurement Algorithms of Selected Electric Parameters in Wide Range of Frequency Change, Proc. of SIP2001, Honolulu, USA, ISBN: 0-88986-297-4, pp. 155-159.

[10] A. Halinka, L. Topór-Kamiński, M. Szewczyk: Analiza dokładności przetwarzania sygnału w torze pomiarowym cyfrowego terminalu automatyki elektroenergetycznej - wybrane wyniki badań, „PAK - Pomiary Automatyka Kontrola 9/2009, Vol. 55”, Wydawnictwo PAK, Warszawa 2009, pp. 769 – 773

[11] A. Halinka, J. Guzik, M. Szewczyk: Wybrane aspekty oceny poprawności pracy przetwornika A/C, procesora sygnałowego oraz innych elementów w torze DSP zabezpieczenia cyfrowego, Przegląd Elektrotechniczny, R. 86 NR 8/2010, pp. 37 – 43

[12] A. Halinka, M. Szewczyk: Badanie wybranych elementów struktury toru przetwarzania sygnału pomiarowego w zabezpieczeniach cyfrowych, Zeszyt tematyczny nr XIII czasopisma „Energetyka” (artykuły I Międzynarodowej Konferencji Naukowo-Technicznej Invention'07 „Innowacyjność w Elektroenergetyce”), pp. 15 - 20, Ustroń, 25-26 październik 2007

[13] IEEE Standard for Synchrophasor Measurements for Power Systems C37.118 rev. 2005

[14] IEEE Standard for Synchrophasor Measurements for Power Systems C37.118.1 rev. 2011

[15] IEEE Standard for Synchrophasor Measurements for Power Systems C37.118.2 rev. 2011

[16] IEEE Standard for Synchrophasor Measurements for Power Systems, Amendment 1: Modification of Selected Performance Requirements, 27 March, 2014

[17] IEEE Std 1588™-2008: IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems

[18] PC37.238 - IEEE Draft Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications

[19] North American Electric Relaibility Corporation (NERC): Time Stamping of Operational Data Logs, Version 0.995, November 11, 2009.

[20] M. Staroń: Time synchronisation in electric power infrastructure – selected issues, Master Thesis supervised by M. Szewczyk.

[21] F. Steinhauser, C. Riesch, M. Rudigier: IEEE 1588 for time synchronization of devices in the electric power industry, Proc. Of 2010 Int. IEEE Symp. on Precis. Clock Synchron. for Meas., Control and Commun., ISPCS 2010; Portsmouth, NH; United States; 29 September 2010 through 1 October 2010, 1-6.

[22] L. Benetazzo, C. Narduzzi, and M. Stellini: Analysis of clock tracking performances for a software-only IEEE 1588 implementation, IMTC 2007, Warsaw, Poland, May 1-3, 2007, 1-6

[23] M. Lixia, C. Muscas, and S. Sulis: Application of IEEE 1588 to the measurement of synchrophasors in electric power systems, ISPCS 2009, Brescia, Italy, Oct. 12-16, 2009, 142-147.

[24] J. S. Warner and R. G. Johnston: A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing, J. of Secur. Adm., 2002, 1-9.B. M. Ledvina, W. J. Bencze, B. Galusha and et al.: An in-line anti-spoofing device for legacy civil GPS receivers", in Proc. of the ION Int. Tech. Meet., San Diego, CA, 2010, 698-712

[25]M. Szewczyk: Time synchronization for synchronous measurements in Electric Power Systems with reference to the IEEE C37.118TM series of Standard – selected tests and recommendations, Przegląd Elektrotechniczny, R. 91 Nr 4/2015, pp. 144-148

[26] M. Chakir, I. Kamwa, H. Le Huy: Extended C37.118.1 PMU algorithms for joint tracking of fundamental and harmonic phasors in stressed power systems and microgrids, IEEE Transactions on Power Delivery, Volume 29, Issue 3, June 2014, Article number 6810880, pp. 1465-1480

[27] A.G. Phadke, B. Kasztenny: Synchronized phasor and frequency measurement under transient conditions, IEEE Transactions on Power Delivery, Volume 24, Issue 1, 2009, pp. 89-95

[28] I. Kamwa, S. R. Samantaray, , G. Joos: Compliance analysis of PMU algorithms and devices for wide-area stabilizing control of large power systems, IEEE Transactions on Power Systems, Volume 28, Issue 2, 2013, pp. 1766-1778

[29] G. Sanchez-Ayala, J.R. Aguerc, D. Elizondo, M. Lelic: Current trends on applications of PMUs in distribution systems, Innovative Smart Grid Technologies (ISGT), 2013 IEEE, vol., no., pp. 1-6, 24-27 Feb. 2013

[30] M. Szewczyk: Wymagania normatywne pomiarów synchronicznych w infrastrukturze elektroenergetyki, Przegląd Elektrotechniczny, R. 90 Nr 3/2014, pp. 80-83

[31] A. Halinka, M. Szewczyk, M. Talaga: Synchronous mesurements techniques (PMU) and sample applications. Wiadomości Elektrotechniczne, 8/2014, R. 82, Sigma-NOT pp. 21-25

[32] A. Halinka, M. Szewczyk, M. Talaga: Possibilities to increase the potential of defense of National Power System using SmartLoad synchronous measurement system. Blackout and the Polish National Power System. Edition 2014: Red. J. Lorenc, A. Demenko. Electrical Science Commission, Poznań Branch of the Polish Academy of Sciences. Ośrodek Wydawnictw Naukowych, Poznań, 2014, pp. 81-89

[33] A. Babś: Rozszerzenie standardu IEC 61850 poza stacje elektroenergetyczne z uwzględnieniem zastosowania w elektrowniach, XVI Seminarium „Automatyka w elektroenergetyce", Zawiercie, 17-19 kwietnia 2013 r., Energotest Sp. z o.o., pp. 1.1-1.13

[34] C. Cardenas, C. De Arriba, A. Lopez De Viñaspre, G. Gonzalo: Zastosowanie i doświadczenie eksploatacyjne z protokołem IEC 61850 XVI Seminarium „Automatyka w elektroenergetyce", Zawiercie, 17-19 kwietnia 2013 r., Energotest Sp. z o.o., pp. 8.1-8.16

[35] M. Szewczyk, A. Halinka: Media transmisyjne i ich wykorzystanie w infrastrukturze teleinformatycznej energetyki, Wiadomości Elektrotechniczne 2007 R. 75 nr 12, pp. 12-15

[36] M. Szewczyk: Teleinformatic structures with reference to the forecasting functions of electric power Smart Grid networks (1), „Elektro.info 5/2014", Dom Wydawniczy MEDIUM, Warszawa 2014, pp. 40-43

[37] M. Szewczyk: Analysis of the requirements of reliability and quality for systems and data transmission equipment in modern power systems, Przegląd Elektrotechniczny, ISSN 0033-2097, R. 90 Nr 3/2014, pp. 84-89

[38] M. Szewczyk: Selected analyses of teletransmission and teleinformatic structures in electrical power, Przegląd Elektrotechniczny, R. 90 Nr 3/2014, pp. 1-5

[39] A. Halinka, M. Szewczyk: Bezpieczeństwo przesyłu informacji oraz algorytmy szyfrujące możliwe do wykorzystania w infrastrukturze teleinformatycznej energetyki, Wiadomości Elektrotechniczne, 6/2008, pp. 3-8

[40] M. Szewczyk: Selected security threats of the teleinformatic structures with reference to the forecasting functions of electric power Smart Grid networks (2), „Elektro.info 7/8/2014", Dom Wydawniczy MEDIUM, Warszawa 2014, pp. 44-46

[41] A. Halinka, M.Szablicki: Metoda estymacji składowych impedancji niewrażliwa na odczepowe przyłączanie źródeł wiatrowych (część 2 – minimalizacja wpływu niezerowej wartości rezystancji przejścia w miejscu zwarcia), Przegląd Elektrotechniczny, R. 88 Nr 9a, 2012, pp. 7-11

[42] M.M. Saha, J. Izykowski, M. Lukowicz, E. Rosolowski: Application of ANN methods for instrument transformer correction in transmission line protection, 7th International Conference on Developments in Power Systems Protection (DPSP 2001), 2001 p. 303 – 306

[43] M. Szewczyk, A. Halinka: Electrical Fault Detection in Power Systems by ANN Structures, WSEAS TRANSACTIONS on SYSTEMS, Issue 4, Volume 3, June 2004, pp. 1681-1685

[44] M. Szewczyk, A. Halinka: Wspomaganie podejmowania decyzji w układach i systemach elektroenergetycznych z wykorzystaniem sztucznych sieci neuronowych część 1, „Elektro.info 4/2005", Dom Wydawniczy MEDIUM, Warszawa 2005, pp. 67 – 72

[45] M. Szewczyk, A. Halinka: Wspomaganie podejmowania decyzji w układach i systemach elektroenergetycznych z wykorzystaniem sztucznych sieci neuronowych część 2, „Elektro.info 6/2005", Dom Wydawniczy MEDIUM, Warszawa 2005, pp. 44 – 50

[46] A. Halinka, M. Niedopytalski: Wykorzystanie niekonwencjonalnych technik decyzyjnych do poprawy działania zabezpieczenia odległościowego linii napowietrznej WN o zmiennych w szerokich granicach zdolnościach przesyłowych. Cz. 1, Przegląd Elektrotechniczny, R. 90 Nr 3, 2014, pp. 10-14

[47] www.westermo.com (documentation of Westermo T208 switch)

[48] www.globalsat.com.tw (documentation of the GPS EM-406A device)

[49] www.energotest.com.pl

[50] www.kaspersky.com

***Author**: dr inż. Michał Szewczyk, Politechnika Śląska w Gliwicach, Instytut Elektroenergetyki i Sterowania Układów, ul. B. Krzywoustego 2, 44-100 Gliwice, E-Mail: Michal.Szewczyk@polsl.pl.*