2018 International Conference on Industrial Engineering, Applications and Manufacturing (ICIEAM)

# Cyber-Security Problems in Smart Grid

## Cyber Attacks Detecting Methods and Modelling Attack Scenarios on Electric Power Systems

Sharafeev T.R., Osokin V.Ju.
Dept. «Power engineering, electricity supply and power electronics»
NSTU n.a. R.E. Alekseev
Nizhniy Novgorod, Russia
sharafeev-94@mail.ru, osokin-v92@mail.ru

Kulikov A.L.
Dept. «Power engineering, electricity supply and power electronics»
NSTU n.a. R.E. Alekseev
Nizhniy Novgorod, Russia
inventor61@mail.ru

***Abstract*—The intellectualization of an electrical power system (EPS) creates a required infrastructure for the efficient transmission, distribution and consumption of electrical energy, and is based on the integration of the EPS with information networks. Significant disadvantages of such integration are related to the problems of cyber security which have become particularly important in recent times. Currently, the applied methods of cyber security are taken from information technology and in no way are connected with the specifics of electrical power systems. The purpose of this article is to develop an algorithm to detect cyber-attacks based on continuous monitoring of the EPS parameters. The method is based on the algorithm of additional authentication of the SV-messages of the IEC 61850 Protocol sent between microprocessor devices of relay protection and automation (MDRPA). This authentication is based on the results of beforehand simulation of many regimes of the analyzed electrical network. Additionally, the authors presented the analysis of the scenarios and damage from cyber-attacks which includes the sequential outages of power generation facilities. The cyber-attack scenario is the result of an iterative calculation of the steady state modes of the electrical network depending on the indices of the elements.**

***Keywords—smart grid; cyber-attacks; cybersecurity; short circuit, scripts; relay protection devices; damage from cyber-attacks; power system***

## I. INTRODUCTION

The intellectualization of electrical power systems (EPS) creates the required infrastructure for efficient transmission, distribution and consumption of electrical energy, and is based on the integration of EPS with information networks [1]. Significant disadvantages of this integration are related to the problems of cybersecurity, which are especially acute in recent times [2]. It should be noted that the electric power industry belongs to a critical infrastructure [3, 12], and its smooth functioning is an important component of economic systems reliability [4].

Unfortunately, the main methods ensuring cybersecurity, which are now used in electrical networks [1, 5], are borrowed from the field of information technologies and are in no way related to the electric power production specifics.

The object of the research is to work out an algorithm based on continuous monitoring of EPS parameters to detect cyber-attacks. Additionally, the analysis of scenarios and damage from cyber-attacks, expressed in consecutive outages of electric power facilities, is carried out.

To carry out research on the topic, an EPS site consisting of 220 kV ring mains supply and 110 kV ring distribution networks was selected (Figure 1). The electric grid complex includes electric substations with autotransformers and transformers, as well as overhead transmission lines. Consumers' power supply comes from two sources: the joint electric power system communicating with the neighboring subsystems in the 220 kV ring and the local TPP in the 110 kV ring. In the course of multiple simulation experiments, the parameters of normal, post-emergency and emergency steady-state operation modes of the electric network were estimated (Figure 1).

To implement cyclic calculations of emergency modes for nodes and branches of the electrical network, a special software in Visual Basic with a graphical interface in the form of a Microsoft Excel spreadsheet was developed. The software uses the loop method to calculate system-fault duty and the nodal potential method to calculate normal conditions.

## II. MATERIALS AND METHODS

### *A. Method of detection a cyber-attack on the power system*

Let the emergency mode, fixed by microprocessor devices of protective relaying and emergency control schemes and ACS TP of substations characterize an actual damage in the power system or a cyber-attack. Taking into account the application of the standard of modern digital sub-stations IEC 61850 [6], SV and GOOSE messages are generated. Protective relaying and emergency control schemes protecting a certain section of the electric network exchange those messages.

When transmitting, in particular, the SV messages between protective relaying and emergency control schemes, there is a violation of the integrity of the data packets [12]. This allows to determine the fact of the presence of an external unauthorized intervention in the information space of the

978-1-5386-4307-5/18/$31.00 ©2018 IEEE

agricultural technological process. If the attacker does not know the principles of the data encryption used in the transmission of messages, the detection of invasion by detecting broken communication packets is highly efficient.

However, if the attacker is aware of the information protection measures in use, and he can substitute (distort) the SV messages transmitted, a false alarm and an unwanted tripping of the power network element will occur. To avoid this situation it is suggested introducing additional authentication of the transmitted SV messages. This verification is based on the use of the preliminary simulation results of the analyzed electrical network emergency modes variety.

*B. The method of cyber-attack scenarios*

The method is based on the anticipating the scenario of a cyber-attack. Guided by the principle that any organized attack on industries (in particular, on agricultural) occurs to cause maximum damage, we can obtain a matrix of attack scenarios when examining a particular electrical network. Time required to detect an attack is determined by the time of the search for the correspondence of the emergency situation to one of the previously simulated scenarios.

To calculate cyber-attacks scenarios, there is used the linearization method of the power system operating mode by representing it in the form of a set of passive (complex resistances) and active (current sources in the nodes) elements [7, 13]. Thus, the load and generation nodes are represented as ideal current sources, in which the signs of the real and imaginary parts characterize the corresponding nodes. Power transmission lines and windings of power transformers are represented simplistically by concentrated complex resistances disregarding mutual induction.

The electrical network is modeled as a directional graph, which is mathematically represented as an incident matrix. The incident matrix of the electric network graph is then used to solve linear equation systems by the Gauss method to determine the voltage vectors at the nodes and currents in the branches.

$$\overline{U} = \left[U_1, U_2, \ldots, U_n\right]^T \quad (1)$$

$$\overline{I} = \left[I_1, I_2, \ldots, I_n\right]^T \quad (2)$$

Where “n” represent number of nodes in electric power grid model.

Expressions (1) and (2) characterize nodes parameters of the electrical networks district model. The voltage is the reference of the criterion for the existence of the mode. The second reference value is the currents in the branches. The transformer ratios for the branches are taken to be valid [11]. The currents in the branches represent a column-matrix.

$$\overline{J} = \left[J_1, J_2, \ldots, J_m\right]^T \quad (3)$$

Where “m” represent number of branches in electric power grid model.

From a mathematical point of view, the problem of calculating the steady-state mode of the electric network model in question belongs to the nonlinear class and, consequently, its solution can be obtained, for example, by iterative methods.

Cyber-attacks scenarios are the results of iterative recalculations of the steady-state mode of a given model of an electrical grid, depending on the elements state indexes [9]. Each scenario consists of groups that correspond to a set of switches [14]. For the model in question, there are used scenario groups containing one shutdown.

The state indexes are calculated as it is required to maintain load nodes (static stability) and preserve the branches in operation in accordance with the maximum permissible current loads.

For the branches state indexes are calculated by the expression:

$$IS_i = \frac{I_{fact,i}}{I_{\max,i}} \quad (4)$$

Where $I_{fact,i}$ represent the modulus of current flowing in the i-branch; $I_{\max,i}$ represent the limit value of the current for a given branch.

The current limit value $I_{\max,i}$ is taken into account in accordance with the following provisions:

- For power lines with any number of circuits, the limiting current is assumed equal to the valid durable current of the line;

- For power transformers and autotransformers, the limiting current in the windings is assumed equal to the current in accordance with their maximum allowable load

$$ISi_j = \frac{K_j \cdot S_j}{\sqrt{3} \cdot U_j} \quad (5)$$

Where $S_j$ is the rated capacity of the power transformer (autotransformer); $K_j$ is the coefficient of transformers (autotransformers) overload capability; $U_j$ - rated winding voltage.

For the nodes, state indexes are calculated by the expression:

$$ISu_j = K_{s.rel,j} = \frac{U_{fact,\mathrm{j}} - U_{\max,j}}{U_{fact,\mathrm{j}}} \quad (6)$$

Where $U_{fact,\mathrm{j}}$ is the actual voltage in the j-load node; $U_{\max,j}$ is the critical voltage of the load node; $K_{s.rel,j}$ is the steady-state stability factor of the load [9].

The critical voltage $U_{\max,j}$ of load nodes is determined by the condition of maintaining a stable work load [9]. In the

calculations, the motor character of the load and the conditions for its stable operation with a change in the voltage at the node are assumed. When the value of the actual voltage on the load decreases by more than 30%, a significant part of the motor load is disconnected. This situation is modeled by changing the value of the total power consumption in the node by 25% compared to the given one. The further decrease of the voltage in the node by more than 40% leads to the final load drop and, consequently, to the disconnection of the node from the power system by protective relaying devices.

Electrical network malfunction is a criterion for exiting the iterative calculations of cyber-attack scenarios. This parameter represents the amount of total electricity shortage to consumers in the electric grid, which is determined by the expression

$$S_{ful} = \sum_{m=1}^{N} n \cdot S_n + \Delta S \qquad (7)$$

Where $S_{ful}$ is the total value of load nodes capacity of the total power of the electric network; $n$ is the number of load nodes under consideration; $\Delta S$ - the amount of additional capacity reserve, which can be brought in by the power system at the time of a cyber-attack.

The first group of scenarios is the deactivation of any schema branches. From the second, the groups are ordered and represent branch outages based on the current state indexes of the network elements (expression 6).

## III. Results

### A. Detection of cyber-attacks on the power system

The application of the developed method is illustrated by the example of line 1 of EPS, presented in Figure 1.

The line has the following features:

- connects the communication node 1 with the power energy system and the 220 kV substation;

- It transmits a large flow of power, so its state significantly affects the reliability of the electrical network.

Normal and emergency modes of the electric network with obtaining current by branches were calculated with developed software [15, 3]. Implementation of the calculations was carried out iteratively. Each iteration was characterized by random parameters of the emergency process: location of the fault point on the line, type of short-circuit and value of the transient resistance [10, 20]. The distribution of currents in the branches with a two-phase short-circuit on line 1 is shown in Figure 2 (a). A similar voltage distribution at the nodes is shown in Fig. 2 (b).

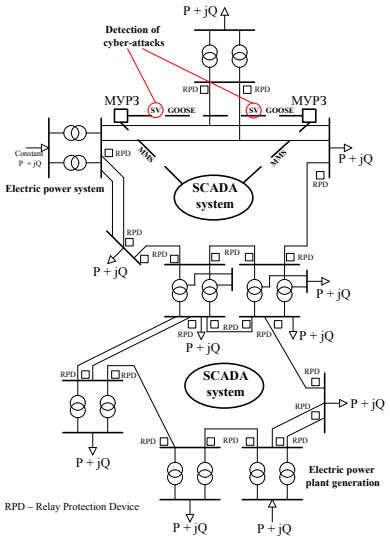


Fig. 1. Electric power network used for modelling and example of cyber-attack detecting method

As the change in the current values in SV messages of IEC 61850 leads to the electric power object relay protection operation, to verify the data a cyclic algorithm which includes the following actions (Figure 3) is developed [5, 19]:

- Selection of the branch of the modeled EPS;

- Formation of a false current value ($I_{ph}$);

- Formation of false voltages ($U_{begin}$ and $U_{end}$);

- Search for current coincidences for emergency modes;

- Comparison of actual voltage in nodes with false ones;

- Conclusion about compliance with the current mode or a cyber-attack.

To generate random false currents in the selected branch ($I_{ph}$);, the nominal branch voltage and the range of currents, from which ($I_{ph}$) was subsequently randomly selected, were determined.

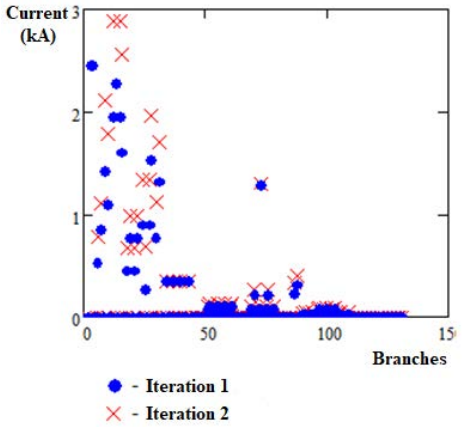


Fig. 2(a). Example of the distribution of parameters in an electrical network with short-circuit mod on line 1 (current in branches

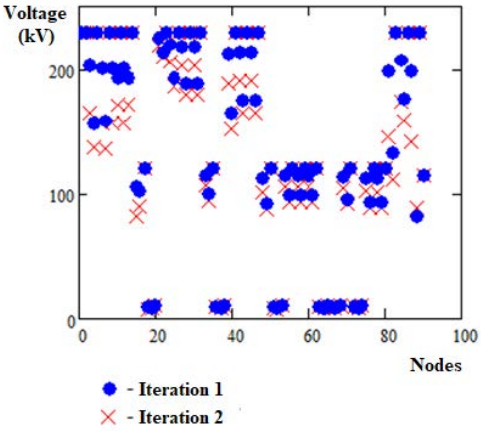


Fig. 2(b). Example of the distribution of parameters in an electrical network with short-circuit mod on line 1 (current in branches

The average value of the current in the i-element of the electrical network was formed according to the expression [16]:

$$I_{mid.i} = \frac{S_{mid.i}}{\sqrt{3} \cdot U_{mid.i.}} \tag{8}$$

In (8) $I_{mid.i}$ represent middle current value in i-branch; $S_{mid.i}$ - middle value of power in i-element of power system model; $U_{mid.i.}$ - middle value of voltage in i-element of power system model.

Voltage values were set to nominal for both power lines and transformers (autotransformers) [19]. In multiple experiments, emergency modes were modeled only on power lines. It was assumed that the probability of a cyber-attack on the primary equipment of an electrical substation is small.

The range of random sampling of false fault currents was determined by the following expressions:

$$\begin{aligned} I_{ph.\min.i} &= K_{\min.i} \cdot I_{mid.i} \\ I_{ph.\max.i} &= K_{\max.i} \cdot I_{mid.i} \end{aligned} \tag{9}$$

Where $I_{ph.\min.i}$ is the value of the minimum falsified current for the i-element of the electric network; $I_{ph.\max.i}$ is the value of the maximum falsified current for the i-element of the electric network; $K_{\min.i}$ is the value of the coefficient determining the lower bound of the range; $K_{\max.i}$ is the value of the coefficient determining the upper limit of the range.

The value of the false voltage of the i-branch was determined by a random sample from $I_{ph.\min.i}$ to $I_{ph.\max.i}$ (expression 9). For the selected branch, the values $K_{\min.i}$ and $K_{\max.i}$ were taken equal to 2 and 57, it means the maximum and minimum

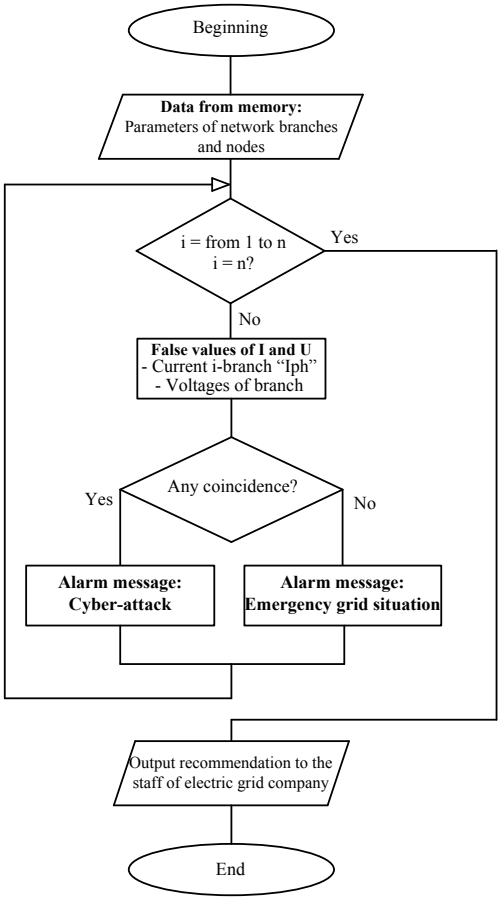


Fig. 3. Generalized block diagram of cyber-attack determine algorithm

values of short-circuit currents on this line, obtained from the analysis of emergency conditions parameters.

Falsified voltages were determined in a simplified manner using Ohm's law. In this case known parameters are the voltages of the initial node (node "F") and the end node of the branch (node "S").

The effective values of these nodes the voltages were determined by the expression (10).

$$\begin{aligned} U_{f.i} &= rand(K_U \cdot U_{mid.i}, U_{mid.i}) \\ U_{s.i} &= U_{f.i} - I_{ph.i} \cdot Z_i \end{aligned} \tag{10}$$

Where $U_{f.i}$ is the value of the fabricated voltage of the beginning of the i-branch; $rand(K_U \cdot U_{mid.i}, U_{mid.i})$ is a function of random sampling from a specified range; $K_U$ is the coefficient of criticality of changes in the voltage of the node (it is taken by chance from the range from 0.7 to 0.8).

A generalized control-flow chart of cyber-attack detection is presented in Figure 3. The algorithm is based on the comparison of real and model data and allows to realize an effective fixation of cyber-attacks. Special software for cyber-attacks detection should be implemented in the form of an automated control subsystem of dispatch control and technological management [7, 12].

### B. *Analysis of scenarios of cyber-attacks*

The purpose of cyber-attacks scenarios analysis was the identification of the most vulnerable elements of the electric network, the input on which leads to the largest number of power cut offs [22]. In addition, the scenarios were investigated for the frequency of repetition for the worst variants of power supply to consumers [18].

The analysis was carried out with simulation modeling, and its results can be used to organize trainings on proper conduct for operational personnel modeling cyber-attacks on the energy system [12, 17]. Potentially vulnerable power system objects, which are typical for the detected cyber-attack scenario, should be disconnected from the general information network and transferred to autonomous (local) management or using direct commands of the power system dispatcher [13].

An example of the control personnel possible decision during a cyber-attack at the EPS (Figure 1) is shown in Figure 4. When the scenarios of attack are detected on branches 34-36 of the modeled EPS, the subsequent threat for branch 44 is clearly visible, therefore, it is recommended to transfer the appropriate network protection and management tools in an autonomous functioning [8, 13].

Statistics of cyber-attacks simulation are given in Figures 5 and 6. In Figure 5, the frequency of repetition of the electrical network elements in the cyber-attacks scenarios [23] is given. In Figure 6, the volumes of the consumers' switched off power (damage) are presented. The peak values of the damage on the graph (Figure 6) correspond to those scenarios [17, 21], when the mode is physically unstable, (the capacity of the entire network does not allow transferring a given amount of power to consumers).

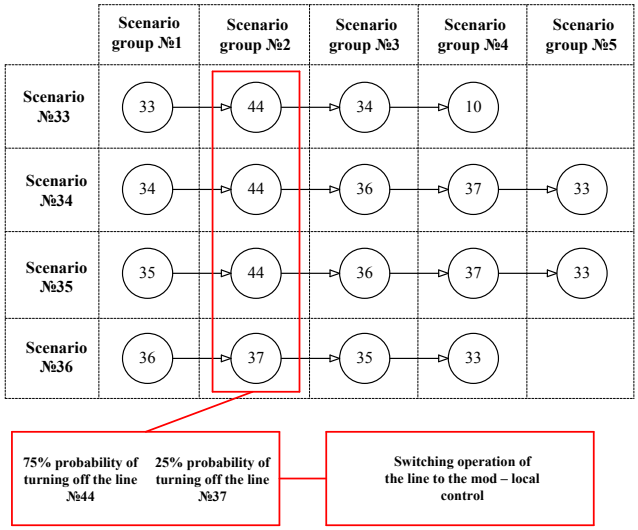


Fig. 4. Example of making a decision during cyber-attack

## IV. Conclusion

1. The creation and development of intelligent electrical networks requires a deep understanding of the potential consequences of the introduction of information technology and the emergence of cyber threats.

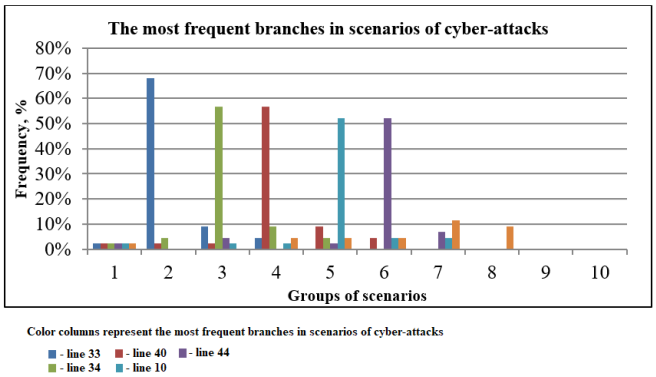


Fig. 5. Example of making a decision during cyber-attack

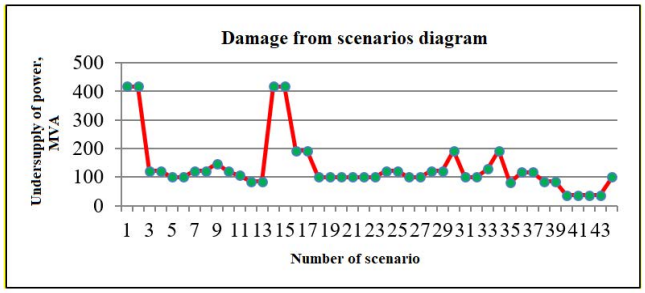


Fig. 6. Damage from scenarios diagram

2. The proposed method for detecting the distortion of SV messages of the protocol IEC 61850, exchanged by microprocessor devices for relay protection and automation, is an effective means of detecting cyber-attacks. The use of statistical data of the simulation model of emergency regimes makes it possible to distinguish the current mode of the electrical network from a cyber-attack.

3. The analysis of cyber-attacks scenarios with the use of simulation modeling provides identification of the most vulnerable elements of the electric network, as well as the definition of the operational personnel behavior strategy in case of information protection violations and minimization of damage from outages.

## References

[1] V.E. Fortova and A.A. Masterova, The concept of Russian intellectual power system with actively adaptive network. Moscow: FSK EES, 2012.

[2] B.V. Papkov, A.L. Kulikov, and V.L. Osokin, Cyber threats and attacks in electric power industry. N. Novgorod: NIU RANKhiGS, 2017.

[3] A.L. Kulikov and V.M. Zinin, “The establishment of cyber security system in the Russian electric power industry considering the implementation of the smart grid concept,” Electricity. Transmission and distribution, no. 5(32), pp. 122-126, 2015.

[4] A.L. Kulikov, “Management of economic relia-bility of farm systems,” Ph.D. Dissertation, N.Novgorod, 1998.

[5] On approval of Requirements for ensuring information pro-tection in automated control systems of production and technological processes at critically important objects, poten-tially hazardous objects and objects of increased danger to life and health of people and the environment, 2014.

[6] On amendments to the Federal law “On electric power industry” in terms of improving the requirements to ensure the reliability and security of electric power systems and of power facilities.

[7] V.A. Kharlamov, “The recovery of power relay sys-tems after successful cyber-attacks,” Relayer, no. 2, p. 54, 2016.

[8] GOST IEC 61850-7-4-2011, Network and communication systems at substationpp. Part 7. Basic communication structure for substations and line equip-ment. Section 4. Compatible logical node classes and data classes.

[9] V.A. Venikov, V.I. Gorushkin, and I.M. Markovich, Electrical calculations, programming and optimi-zation of power system modes. Moscow: Vysshaya shkola, 1973.

[10] Yu.A. Fokin and A.M. Khozyainov, “The input mode of electric power systems in the acceptable region by adjusting their schemes,” Electricity, no. 12, pp. 14-19, 1990.

[11] K.D. Anisimova, V.A. Venikov, V.V. Ezhkov, The method of calculation of stability of automated electrical systems. Moscow: Vysshaya shkola, 1966.

[12] NERC Critical Infrastructure Protection (CIP) Reliability Standards, North American Electric Reliability Corporation, 2009.

[13] D. Kundur, X. Feng, P.P. Liu, T. Zourntos, and K. Butler-Purry, “Towards a framework for cyber attack impact analysis of the electric smart grid,” Proc. 1st IEEE Int. Conf. Smart Grid Commun., pp. 244-249, 2010.

[14] P. Mohajerin Esfahani, M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, “Cyber attack in a two-area pow-er system: Impact identification using reachability,” Proc. Amer. Control Conf., pp. 962-967, 2010.

[15] PP. Sridhar and G. Manimaran, “Data integrity attack and its impacts on voltage control loop in power grid,” Proc. IEEE Power Energy Soc. General Meeting, Detroit, 2011.

[16] X. Jin, J. Bigham, J. Rodaway, D. Gamez, and C. Phillips, “Anomaly Detection in Electricity Cyber Infrastructures,” Proc. Int. Workshop CNIP 2006, 2006.

[17] J. Smith, N. Kipp, and D. Gammel, “Defense in Depth Security for Industrial Control Systems,” Proc. of the Electricity Engineers’ Association Conference and Exhibition, 2016.

[18] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, “A survey on cyber security for smart grid communications,” Communica-tions Surveys and Tutorials, IEEE, vol. 14, no. 4, pp. 998-1010, 2012.

[19] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” ACM Transactions on Information and System Security, vol. 14, no. 1, May 2011.

[20] L. Xie, Y. Mo, and B. Sinopoli, “False data injection attacks in electricity markets,” IEEE Int. Conf. on Smart Grid Communications, Brussels, Belgium, Oct. 2011.

[21] Y. Mo, T. Kim, K. Brancik,D. Dickinson, H. Lee, A. Perrig and B. Sinopoli, “Cyber–physical security of a smart grid in-frastructure,” Proceedings of the IEEE, 100(1), pp. 195-209, 2012.

[22] V.Yu. Vukolov, “Improvement of calculation of standards of technological losses of electricity,” Newsletter NGIEI, no. 12 (19), pp. 32-41, 2012.

[23] V.Yu. Vukolov, A.L. Kulikov, and B.V. Papkov, “Locations disconnection of electrical distribution networks using syn-chronized measurements,” Actual problems of reliability of energy systems, pp. 183-189, 2015.