# Vulnerability Analysis of the State Estimation Problem under Cyber Attacks on WAMS

Irina Kolosok, Elena Korkina, Liudmila Gurina
Department of Electric Power Systems
Energy Systems Institute, ESI SB RAS
Irkutsk, Russia
kolosok@isem.sei.irk.ru

***Abstract* – Electric power system is a critical infrastructure and loss of its resilience and/or operability can lead to negative consequences for the national economy. Modern power systems based on sophisticated computer and communication technologies are characterized by elevated vulnerability to different types of unauthorized malicious access, i.e. cyber-attacks. Wide area measurement system which is based on the technology for vector measurements with phasor measurement units refers to the subsystems of electric power systems which are the most vulnerable in terms of the aftermath of cyber attacks. In their earlier researches, the authors of the paper suggested a technique for a two-level distributed state estimation based on singling out the areas in the scheme of electric power systems which are monitored using PMU. The PMU measurements coming at a high frequency make it possible to implement fast linear algorithms of state estimation for such areas. The paper will present potential consequences of cyber attacks on WAMS, their impact on the quality of measurements coming to the state estimation problem and use of distributed state estimation algorithms for their identification.**

***Index Term* – WAMS, PMU measurements, state estimation, cyber attacks, test equation method, bad data detection.**

## I. Introduction

The adoption of complicated technical equipment and advanced information and communication technologies to establish an intelligent power system (IPS) increases the vulnerability of the entire intelligent power system and its individual infrastructures to various failures and disturbances, including those malicious, or cyber attacks.

State estimation is a mathematical method for data processing which makes it possible to calculate state variables of the electric power system on the basis of measurements, and filter gross errors in them. The results of state estimation form the basis for real-time and emergency control of electric power systems, their visualization raises the awareness of the dispatching staff on the current state of electric power system. The most vulnerable in terms of cyber attack consequences for state estimation are the facilities of the information-communication control subsystems, such as SCADA and WAMS, since the input data used for solving the state estimation problem are represented by the SCADA measurements (telemetry and remote signals) and phasor measurements received from the phasor measurement units, which is the main measuring equipment of WAMS. Due to cyber attacks on the SCADA and WAMS, measurement data coming to the state estimation problem are distorted. If no special measures are taken to identify these distortions and suppress their impact on the state estimation results, serious errors can appear in decisions made by dispatchers using the state estimation results. Therefore, to obtain quality state estimation results, the used measurements should be tested for the presence of bad data.

Solutions to the state estimation problem can be considerably improved by combining the SCADA and WAMS measurements. The addition of PMU measurements makes it possible to improve observability of a complete calculated scheme, enhance the efficiency of the methods for bad data detection in the measurement data, and accuracy of the obtained estimates. The measurements from WAMS are assumed to be accurate and reliable. At the same time the research and experience of PMU operation indicate that there can be different reasons for a failure in PMU operation and bad data in their readings. As is shown in a number of publications WAMS can be a potential target for cyber attacks, since to improve state estimation procedure it will be integrated with the SCADA system.

In this paper consideration will be given to potential cyber attacks on WAMS, their impact on the quality of measurements coming to the state estimation problem and on the state estimation results, as well as the use of bad data detection methods for their identification and suppression. The paper is structured as follows. Section II defines three infrastructures representing the links of a system for intelligent power system operation control and their vulnerability to cyber attacks. Section III considers the variants of cyber attacks on WAMS, whose consequences affect the reliability of the state estimation problem. Section IV focuses on the state estimation problem statement and algorithm for the detection of a cyber attack on WAMS by the state estimation methods. Section V suggests the implementation of this algorithm based on PMU measurements.

## II. Cyber Security of Electric Power System. The Most Vulnerable Subsystems

Electric power system is a critical infrastructure and the loss of its resilience and/or operability can result in negative consequences for the national economy. To study the cyber security problems, it is sensible to divide the electric power system into two subsystems, control and

controlled, and consider it as a two-level model. The control subsystem includes the systems of SCADA/EMS, WAMS (Wide Area Monitoring Systems), WAPS (Wide Area Protection Systems), and WACS (Wide Area Control Systems), i.e. information communication infrastructure. The controlled subsystems are represented by the objects of control (electric power plants, substations, transmission and distribution networks), i.e. physical infrastructure.

The comprehensive approach to understanding the security problem of electric power system should employ the notion of a cyber- physical infrastructure [1] which represents the interconnection of information-communication and physical infrastructures.

To develop measures to ensure cyber security of electric power system it is necessary to determine the cyber vulnerability of the considered infrastructures, taking into account their interdependence, analyze the impacts and potential consequences due to the cyber attacks.

A cyber attack on the information-computation subsystem can result in a failure of any component in the measurement, computation and communication systems. Actions of the intruders can weaken the information-communication subsystem, lead to the data loss or unreliability, implementation of negative control actions, etc. Attacks on the information communication infrastructure can cause emergency conditions of the physical system.

In turn, failure of a component of the physical infrastructure can lead to the emergency conditions in the electrical part and facilitate failure of the control system of the information – communication infrastructure [2].

Malicious intrusion in the cyber - physical infrastructure can violate the operability of the information-communication infrastructure and physical infrastructure or of both of them.

With a growing use of information and computation devices in the information-communication infrastructure, its vulnerability to cyber attacks will increase. Therefore, it is necessary to identify potential cyber attacks on the control system and methods for their identification to prevent manipulation of the electric power system control. In this research we have analyzed the vulnerabilities and weaknesses of the information-communication infrastructure in case of cyber intrusions in terms of the state estimation results on the basis of WAMS measurements.

## III. WAMS AND STATE ESTIMATION PROBLEM. POTENTIAL CYBER ATTACKS

### *A. WAMS architecture*

The Wide-Area Monitoring System represents a set of recorders of synchronized phasor measurements (PMU), phasor data concentrators (PDC), channels for data transfer among the recorders, data concentrators and dispatching centers of the JSC "SO UES", as well as systems for processing the obtained information. WAMS measurements are synchronized by the systems of GPS/GLONASS. The hierarchical architecture of WAMS [3] is presented in Fig. 1.

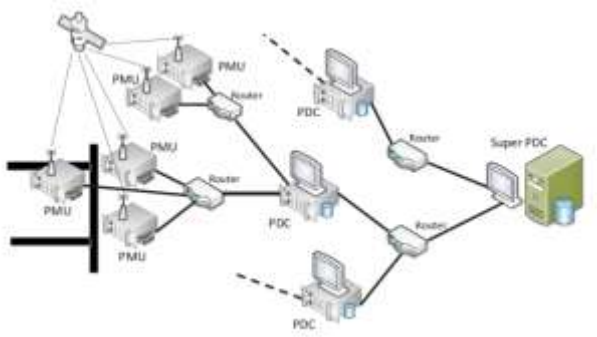


Figure1. Hierarchical architecture of WAMS

Phasor measurement units measure the magnitudes and phases of nodal voltages and currents in lines, which are incident to these nodes. PDC collects, filters, processes and retransmits the data. Besides, PDC can register abrupt surges, distortions, parameters of switches, parameters of loads and lines, and identify generator parameters.

Super-PDC processes data and provides a dispatcher or an operator with graphical interface and access to the data archive.

The existing SCADA measurements and PMU measurements duplicating them make some energy companies think that WAMS are not a strategically important system and technical means of WAMS are not cyber critical components of the energy infrastructure. However, WAMS is vulnerable to cyber attacks.

### *B. Potential cyber attacks on WAMS*

Analysis of potential cyber attacks [4]-[6] has shown that the greatest harm to WAMS can be done in the following way**:**

*1) The devices of PMU, PDC and communication infrastructure proper:*

- **Reconnaissance attacks** allow an adversary to identify weaknesses and potential targets in the WAMS architecture. The aim of these attacks can be the identification of IP addresses of connected PMUs and PDCs. This information can be used for future attacks on WAMS.
- **Communication links damage.** Some companies use overhead fiber optic lines as the main communication lines of WAMS. They are installed in parallel to transmission lines. Therefore, they are exposed to the attacks like cut-off (loss of line connection).

2) *Integrity, accessibility and reliability of data:*

- **False data injection.** sensor measurement injection and command injections. The false data injection attacks can be directed against one or several PMUs, as well as against PDC which receives the flows of synchronized data from several PMUs and forms a single output flow. This makes the PDC an ideal target for the intrusion in order to manipulate a large amount of synchronized measurements afterwards.
- **Denial-of-service attacks.** Denial of service (DoS) can stop the transmission of PMU measurements to the control centers, and the

transfer of control actions, or both. The DoS attack can generate redundant data which will result in traffic overload and in depletion of resources of a most important communication line or router. In this case, the measurements can have a long communication delay or be even denied by a router. Moreover, the denial-of-service attack can terminate the operation of PMU, PDC and super-PDC. For WAMS, this means loss of power system observability.

3) *Reliability of GPS*. Some cyber attacks are designed to do harm to GPS. These are desynchronization, and forced shift of measurement phase from the real value. The authors of [7] show that the GLONASS hardware is extremely vulnerable to the impact of interfering signals, which create a background (masking interference) as well as an intelligent impact (simulating interference). Here there can be some shift of the system time in the PMU devices which may lead to wrong actions of personnel and even disconnection of certain components or emergency islanding of the network. Vulnerability of GLONASS leads to misinformation through the replacement of an accurate time instant by a random time instant during and intelligent attack. In [7] the authors suggest developing software for the GLONASS receivers to detect and exclude simulation interference.

- **Spoofing attacks.** Spoofing attacks are aimed at the GLONASS/GPS synchronization systems. An attacker can perform these attacks to synthesize and transfer fake GPS signals.
- **Replay attacks.** An intruder records valid GPS signals, and transmit them with a delay as corrupted signals, i.e. the information of direct retransmission is distorted.
- **Jamming.** Intruder transmits high-power interfering signals in the GPS frequency band to prevent nearby GPS receivers from receiving and monitoring GPS signals. The authors of [7] say about low immunity of GLONASS/GPS synchronization systems to interference which can be taken for real signals.

The specific feature of technological control in the modern electric power system is imperative transmission of large data volumes to the upper levels of control. Normally, the data are transmitted through the corporate network, but recently the points of interface with the Internet have appeared which makes the network more accessible and thus vulnerable. In some cases it is suggested to apply cloud technologies, particularly in WAMS, for collection and transmission of synchronized vector measurements from the PMU level to the PDC and super-PDC level. With a constantly growing number of cyber attacks on the information structure of energy facilities, the authors of [8] suggest enhancing their cyber security through a reduction in visible zones of potential attacks with the methods of traffic engineering, the development of the next generation commercial anti-viruses and systems to detect the intrusion and block network attacks, and detect the emergence of new network devices.

*C. Technical and information vulnerability of state estimation problem and its information environment*

State estimation is a traditional technique for detecting and suppressing bad data. However, if the attacks are more complicated or more resources turn out to be attacked, this method will not be effective.

Research in [9] shows that if an adversary has a comprehensive idea of the power system topology and values of transmission line conductance, he can attack by injecting false data in such a way that the attack remains unnoticed. In this case, the tests which are normally used in the electric power system state estimation to detect bad data on the basis of discrepancy analysis cannot detect these data.

The study presented in [3] demonstrates that the state estimation using only PMU requires a network where PMU data are adequately delivered in less than 30 ms from all PMUs to PDC and super-PDC which sorts the data according to the time stamp and transmits them to estimators. The authors of [3] have made a considerable contribution to the research into the consequences of cyber attacks on the state estimation procedure: they use a two-module simulation system (PSLF&NS2) to consider a physical damage of the network cable; simulate launch of DoS by blocking network traffic with the routing device overload; present a man-in –the-middle attack where the adversary intercepts the PMU data packets and replaces them with fake data, which leads to wrong state estimation. The simulation results show that: 1) the emergency in a line can make the system unobservable; 2) in case of a routing device failure, the state estimation behavior becomes unstable; 3) the state estimation based on PMU measurements is robust against single PMU data spoofing.

Some papers addressing cyber attacks [3,10,11] show that the communication network is exposed to such attacks as denial of service, replay attack, interference in the operation of sensors or recorders. For the state estimation problem, such events mean the failure to receive data corresponding to the current time instant. In this situation in SCADA systems using telemetry, previously the remote meters marked certain measurements as invalid or the entire snapshot –as a failed snapshot. In the case of a failed snapshot, the state estimator was not started, hence the diagnostics could be seen in the snapshot archives. It is necessary to envisage the same kind of marking the failed snapshots which are formed at the level of PDC and super-PDC in WAMS, and accordingly, not to start state estimation during the whole period of technical faults.

Another type of cyber attack is false data injection in the state estimation problem, when there are no failures in the communication network. If such information comes from single recorders, the state estimator can cope with this problem independently, by a priori finding an erroneous measurement and by replacing it with pseudo measurement. In this case, if the state variable is assigned a fake value (spoofing attack), this value can be identified as systematic error of measurement. However, the time of cyber attacks can be short and hence insufficient to identify such a systematic error. Moreover, a “properly” built attack on

recorder will generate another incorrect value, randomly differing from the previous one. Therefore, the effort to localize the systematic error in the erroneous measurement in order to diagnose the attack manifestation will not always be successful.

In the case where the attack is carried out on a large number of recorders, the number of erroneous measurements can lead to the situation where the computational process of state estimation does not converge. A simple check before state estimation of whether or not the current measurements lie within some technological limits can immediately diagnose if the information failure has occurred. In the state estimator settings it is envisaged to block a large number of errors, thus it is possible to avoid the state estimator start which will lead to a failure in its performance. A great number of rejected measurements can make the system unobservable for state estimation. Problem planner of the computational environment should have a feedback with the state estimator, i.e. the state estimation launch is cancelled in the event that the indicator becomes nonzero. One of the measures to withstand the loss of observability by state estimation is to add WAMS recorders at the energy facility, where in case of rejection of certain measurements they can be replaced by the values calculated by a backup PMU.

## IV. Analysis of Cyber Security of State Estimation Problem at Cyber Attacks at WAMS

Currently, there are algorithms for solving the problem of state estimation using only PMU or only SCADA measurements, or a combination of both.

The analysis of the main algorithms based on the combination of SCADA and PMU measurements shows that they have the main drawbacks characteristic of the traditional state estimation [12]. Therefore, the main attention of researchers and practitioners is paid now to the state estimation algorithms based on the PMU measurements only.

If there is a sufficient amount of phasor measurement units to provide observability of the electric power system scheme, state estimation can be performed using PMU data only. The vector of measurements in this case has the form:

$$\bar{y} = \{\delta_i, U_i, I_{ij}, \varphi_{ij}\}, \quad (1)$$

where $U_i, \delta_i$ – magnitudes and phases of nodal voltages, $I_{ij}$ – magnitudes of currents in branches and $\varphi_{ij}$ – angles between the currents in a branch coming to the *i*-th node and voltage of this node. In addition to these measurements, PMU can calculate active $P_{ij}$ and reactive $Q_{ij}$ flows in the branches. Some PMUs instead of angles $\varphi_{ij}$ measure phase angles of currents $\psi_{ij}$. These angles are connected by the relation: $\varphi_{ij} = \delta_i - \psi_{ij}$ .

When the state estimation problem is solved in rectangular coordinates the model of measurements $\bar{y} = y(x)$, where $x = \{U_{ai}, U_{ri}\}$ is a state vector, becomes *linear*. The state vector estimates can be obtained in one iteration. Thanks to considerably higher accuracy of PMU measurements compared to the traditional measurements, the accuracy of estimates increases.

Unfortunately, modern electric power systems even in the most developed countries are still insufficiently furnished with phasor measurement units to perform linear state estimation for the entire scheme. The algorithms of distributed state estimation on the basis of SCADA and PMU are promising in terms of their practical application. The main idea of such algorithms consists in the following: local areas which are completely observed using PMU measurements are singled out in the scheme of electric power system, and based on linear algorithms local state estimation is performed for these areas. Then, the obtained estimates are transmitted to the dispatching office of electric power system, where the state of the entire system is estimated using SCADA measurements in the rest of the scheme.

The advantages of the local linear state estimation based on the PMU data are obvious. However, there are pitfalls related to the difficulties in detecting bad data in such measurements, which can be caused, in particular by cyber attacks on WAMS.

As the authors of [13] show, loss of synchronization is most unfavorable in terms of impact on the state estimation results. It can be caused by cyber attacks or interference to GPS receiver, or by external problems with synchronization due to computational load of measurement devices, which leads to a delay in the angle measurement. It is important to note that if an angle shift occurs in some PMU channel, this shift occurs in all phase channels. This happens because all phase channels use one and the same GPS time signal and identical code of processing the numerical signal. The same research shows that bad data in the measurements of phase angles of current and voltage are not identified by the traditional methods for the analysis of estimation residuals and, hence cyber attacks aimed at loss of synchronization will not be detected.

One more problem is the propagation of bad data when measurements are converted from polar to Cartesian coordinates [14]. In case of synchronization loss and emergence of bad data in phase angles of voltage and current all four measurements $U_{ai}, U_{ri}, I_{aij}, I_{rij}$ in Cartesian coordinates will be erroneous. The authors of [15] show that the PMU measurement form which is the most resistant to synchronization losses is the voltage magnitude and phase, and the pseudomeasurements $P_{ij}, Q_{ij}$ calculated using the PMU measurements.

In this paper we suggest using the method of test equations to analyze validity of PMU measurements. The method was developed to detect bad data in SCADA measurements [15], then adapted to check the PMU measurements and analyze cyber security of SCADA [16, 17].

Test equations are the steady state equations which include only measured state variables *y*

$$w_k(y)=0 \quad (2)$$

Test equations are used to carry out a priori validation of remote measurements. Substitution of values of measurements in these equations leads to the discrepancy, by comparing which with the threshold $d$, i.e. checking the condition

$$|w_k| < d, \quad (3)$$

we can judge whether or not the measurements that belong to this test equation are valid.

Since the test equation method is an a priori validation method which operates prior to the state estimation algorithm, i.e. calculation of estimates, any representation form of PMU measurements can be used to implement it.

A great variety of steady state equations including PMU measurements makes it possible to use the equations which contain only measured variables at once as test equations. The second approach is to convert PMU measurements into pseudo measurements of active and reactive power flows in branches. Depending on the validation results the vector of measurements for local state estimation of an area is formed

Moreover, up to date the SCADA and WAMS are independent of one another. Therefore, if a local area or an object are observable with WAMS measurements, they are as a rule observable with SCADA measurements as well. Therefore, we suggest, when needed, performing a single (by one timestamp) independent test for validity and state estimation based on SCADA and WAMS measurements to additionally find out if there is a malicious impact on one or another system.

## V. Test of the Suggested Technique in a Simulation Experiment

To do calculations based on the suggested technique we use a fragment of a real network observable by PMU measurements (Fig. 2). The fragment includes two 750 kV lines that have a common node. There are 4 PMUs at the ends of the lines and a PDC installed at node 1 common for them.

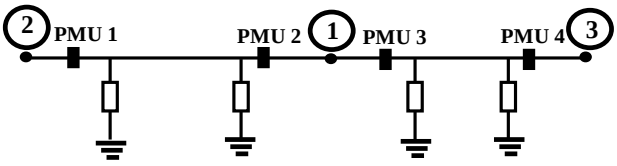


Figure 2. A 3-node scheme consisting of two 750 kV lines

The calculations were done in the simulation experiment when the PMU measurements were simulated by distorting the parameters of the steady state calculation.

The following types of cyber attacks were simulated:

**False data injection** (attack 1) was simulated by the technique presented in [4]. A man-in-the-middle attack on the node was simulated to inject wrong measurements in the data. This node intercepted and modified the C37.118 block of data which were transmitted from PMU-2 to PDC, by doubling the value of all captured vector measurements. The PDC receiving the data failed to distinguish changed packets from unchanged ones. Moreover, the process of changing the data occurred according to the requirements for PDC data frame life time, therefore the changed packets were not marked as old and passed in the state estimator.

**A denial-of-service attack** (attack 2) was simulated by the situation where the measurements did not arrive at PDC. This did not lead to the observability loss but considerably reduced redundancy of PMU measurements, which decreased the efficiency of the bad data detection algorithm.

**Desynchronization attack** (attack 3) was simulated by changing the phase voltage angle at PMU-4 by 9 degrees, which corresponds to missing one point when taking 40 readings in one 50 Hz cycle. Such a distortion of voltage angle led to a distortion of measurements in other angles: the angle of current in branch 3-4 and load angle at the node of PMU placement.

Table 1 presents the state estimation results based on the data exposed to attacks, and measures undertaken by the state estimation methods to detect such data.

**A comment on attack 3:** as was said above if an angle shift occurs in a certain PMU channel, the same shift will happen in all phase channels. Therefore, the same shift in the voltage angle $\delta_3$ and current angle $\psi_{31}$ will not affect the angle between voltage and current vectors $\varphi_{31}=\delta_3-\psi_{31}$, hence, this error will not change the values of active and reactive power. In this case, if the neighboring PMU gives a valid angle measurement, then $\delta_3$ will be calculated correctly.

## VI. Conclusions

1. The wide area monitoring system (WAMS), which is based on the technology for vector measurements using PMUs, is one of the most vulnerable subsystems of intelligent energy system in terms of cyber attack effects.
2. The state estimation results underlie the real-time and emergency control of electric power system. Linear state estimation of local areas observed with the PMU measurements is a promising direction in the development of state estimation methods.
3. The potential cyber attacks on WAMS have been analyzed. They cause the greatest damage to the measurement data coming from PMU. It is shown that the procedures for a priory detection and compensation for erroneous measurements are an effective tool for the identification of technical failures and malicious attacks on WAMS, and elimination of their impact on the state estimation results.

TABLE I. DETECTION OF AN ATTACK BY STATE ESTIMATION METHODS

| | Measurement U – kV; I – kA; P – MW; Q - Mvar | Reference $y_0$ | Measurement $\bar{y}$ | State estimation results | | | |
|---|---|---|---|---|---|---|---|
| | | | | Value of measurement at attack $y_{att}$ | Detection of attack by the state estimation methods | Corrected measurement $\bar{y}_{new}$ | Estimate $\hat{y}$ |
| **Attack 1** | $U_2$ | 773.4 | 773.5 | 1547 | $U_2$ exceeded the limits | excluded | 773.7 |
| | $\delta_2,^\circ$ | 79.2 | 79.3 | 79.2 | 79.2, valid | 79.2 | 79.2 |
| | $P_{21}$ | 983 | 979 | 3960 | $\bar{P}_{21}$ exceeded the limits, replaced: $P_{21} = P_{12} - \Delta P_{12}$ | 990 | 990 |
| | $Q_{21}$ | -319 | -315 | -1260 | $\bar{Q}_{21}$ exceeded the limits, replaced: $Q_{21} = Q_{12} - \Delta Q_{12}$ | -320 | -320 |
| **Attack 2** | $U_1$ | 756,4 | - | No | $U_1 = f_1(U_2, I_{21}, \delta_2)$ | 754.6 | 754.6 |
| | $\delta_1,^\circ$ | 68,4° | - | No | $\delta_1 = f_2(U_2, I_{21}, \delta_2)$ | 68.7 | 68.7 |
| | $P_{12}$ | -972 | -970 | No | $P_{12} = f_3(U_1, I_{12}, \varphi_{12})$ | -968.8 | -972 |
| | $Q_{12}$ | -360 | -362 | No | $Q_{12} = f_4(U_1, I_{12}, \varphi_{12})$ | -360.3 | -365 |
| | $P_{13}$ | 1851 | 1850 | No | $P_{13} = f_3(U_1, I_{13}, \varphi_{13})$ | 1848 | 1850 |
| | $Q_{13}$ | -42 | -40 | No | $Q_{13} = f_4(U_1, I_{13}, \varphi_{13})$ | -42 | -42 |
| **Attack 3** | $U_3$ | 750.3 | 750.4 | 750.4 | 750.4, valid | 750.4 | 750.4 |
| | $\delta_3,^\circ$ | 61,9° | 61,9° | 70,9° | Error is detected by the test equation $\delta_j^{pacч} = \delta_i - arctg \frac{I_{ij}(x_{ij}\cos\varphi_{ij} - r_{ij}\sin\varphi_{ij})}{U_i - I_{ij}(r_{ij}\cos\varphi_{ij} + x_{ij}\sin\varphi_{ij})}$ | 61,9° | 61,9° |
| | $P_{31}$ | -1835 | -1835 | -1835 | -1835 | -1835 | -1835 |
| | $Q_{31}$ | -12 | -12 | -12 | -12 | -12 | -12 |


## ACKNOWLEDGEMENT

The research was supported by grant 4711.2014.8 of Leading Scientific School of the Russian Federation


## REFERENCES


[1] S. Sridhar, A. Hanh, M. Govindarasu, "Cyber-Physical System Security for the Electric Power Grid", *Proceeding of the IEEE*, vol. 100, pp. 210-224, Jan. 2012.

[2] Voropai N.I., Domyshev A.V., Nepomnyashchy V.A., "Models and methods for the research into the security of electric power systems," in *"Reliability of energy systems: problems, models and methods for solving them,"* Novosibirsk: Nauka, 2014, p. 57-74.

[3] Hua. Lin, Yi Deng, Sandeep Shukla, James Thorp, Lamine Mili, "Cyber Security Impacts on All-PMU State Estimator – A Case Study on Co-Simulation Platform GECO", in *Proc. 5-8 Nov. 2012 Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conf.*, pp. 587-592.

[4] T.H. Morris, P. Shengyi, U. Adhikari, Cyber Security Recommendations for Wide Area Monitoring, Protection and Control Systems, in *Proc.22-26 July 2012 IEEE Power and Energy Society General Meeting*, pp.1-6.

[5] Liang Heng, Jonathan J. Makela, Alejandro D. Dom´ınguez-Garc´ıa,Rakesh B. Bobba, William H. Sanders, and Grace Xingxin Gao, "Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture," in *Proc. 2014 Power and Energy Conference at Illinois (PECI)*, pp. 1-7.

[6] Mohd Rihan, Mukhtar Ahmad, M. Salim Beg, "Vulnerability Analysis of Wide Area Measurement System in the Smart Grid, " *Smart Grid and Renewable Energy* [Online], Sep. 2013, pp. 1-7.Available: http://www.scirp.org/journal/sigre

[7] Nudelman G.S., Oganesyan A.A., "About protection of synchronization systems using GLONASS/GPS signals from intelligent interference impact," in *Proc. of XXII Conference "Relay Protection and Automation of Energy Power Systems,"* Moscow, May 27-29, 2014, pp. 427-431.

[8] Nikandrov M.V., Braguta M.V., "Cyber threats to the control systems of modern substation," in *Proc. of XXII Conference "Relay Protection and Automation of Energy Power Systems,"* Moscow, May 27-29, 2014, pp. 424-426.

[9] Md. Ashfaqur Rahman and Hamed Mohsenian-Rad, "False Data Injection Attacks with Incomplete Information Against Smart Power Grids," in *Proc. 2012 IEEE GLOBECOM*, pp. 3153-3158.

[10] S. Sridhar, A. Hahn, M. Govindarasu, "Cyber Attack-resilient Control for Smart Grid," in *Proc. 2012 IEEE ISGT*, Washington, USA, pp.1-3.

[11] C. Beasley, G. Kumar Venayagamoorthy, and Richard Brooks, "Cyber Security Evaluation of Synchrophasors in a Power System," *in Proc. 13th Clemson University Power Systems Conference*, 2014.

[12] Kolosok I., Khokhlov M., "Specific Features of State Estimation Problem in Control of Electric Power System with Active-Adaptive Properties," in *Proc. of the 5th Intern. Conf. "Liberalization and Modernization of Power Systems: Smart Technologies for Joint Operation of Power Grids"*, Irkutsk, Russia, Aug. 6-10, 2012.- P.100-108.

[13] Luidi Vanfretti, Joe H. Chow, "Synchrophasor Data Application for Wide Area System," in *Proc. of the 17th Int. Power System Computation Conference PSSC-2011*, Stockholm Sweden-August 22-26, 2011.

[14] Khokhlov M., "Identifiability of errors in synchronized vector measurements," in *Proc. of Conference "Modern approaches to ensuring the electric power system reliability*," Syktyvkar: Komi RC UB RAS, 2014, pp.88-96.

[15] Gamm A.Z., Kolosok I.N., "Test Equations and Their Use for State Estimation of Electrical Power System," in *Proc of Conf. "Power and Electrical Engineering: Scientific Proc. of Riga,"* Technical University. Riga: RTU, 2002, pp. 99-105.

[16] Glazunova A.M., Kolosok I.N., Korkina E.S., "Study of test equations method's application for bad data detection in PMU measurements," in *Proc. of PMAPS 2012*, Istanbul, Turkey, June 10-14, 2012, #106.

[17] I. Kolosok, L. Gurina, "Calculation of Cyber Security Index in the Problem of Power System State Estimation Based on SCADA and WAMS Measurements," in *Proc. of 9th International Conference on Critical Information Infrastructures Security*, October 13-15, 2014, Limassol, Cyprus, ID 12.