Application of the state estimation procedure to improve the cyber-physical stability of the smart grid

Irina Kolosok*, *Elena* Korkina, and *Ivan* Demidov

Melentiev Energy Systems Institute Siberian Branch of Russian Academy of Science, 664033 Irkutsk, Russia

Abstract. Current Smart Grids and their facilities acquire stable features of cyber-physical systems, the components of which are physical (technological) and information - communication subsystems. In a cyber-physical system, a failure in one subsystem can cause a failure in an other one, and combined emergency states can occur as a result, so there is a problem of ensuring the Smart Grid resilience to physical and information disturbances - the problem of cyber-physical stability (resilience). The report considers the issues of applying the State Estimation procedure to analyze and increase the resilience of Smart Grid and its facilities. It is shown that the State Estimation procedure serves as an effective mean of identifying deliberate impacts or cyber-attacks on the information-communication subsystem and eliminating their consequences on technological subsystem operation. Ways to improve the efficiency of the State Estimation procedure for solving this task are considered.

1 Introduction

The development of the Russian electric power industry, based on the concept of Smart Grids, leads to a radical change in the structure and properties of power systems, giving rise to new problems in their functioning. Modern electric power systems (EPS) are acquiring stable features of cyber-physical systems (CPS), the components of which are the physical and information and communication subsystems. As the EPS "digitalizes", both subsystems become equally complex, equally significant and significantly influencing each other. The introduction of complex technical, information and communication equipment leads to an increased vulnerability of the Smart Grids as a whole and its individual subsystems to various failures and disturbances, including deliberate ones. Therefore, at present, when developing conceptual models and projects for the development of EPS, much attention is paid to the problem of ensuring cyber-physical stability, i.e. stability of the Smart Grid and its objects to physical and information disturbances [1-5].

The most vulnerable and dangerous in terms of the consequences of realized failures, disturbances, deliberate actions or cyber attacks for Smart Grids are the objects of the information and communication control subsystem, such as SCADA systems that collect telemetry data, Wide Area Measurement System (WAMS), registering Synchronized Phasor Measurements (SPM), Wide Area Control System (WACS), etc. [6,7].

As a result of cyber-attacks on SCADA and WAMS aimed at distorting or stealing data, the tasks of managing the technological subsystem (TS) may receive distorted information about the operating parameters. If special measures are not taken to identify these distortions, serious errors may occur in the decisions made during the dispatching control of the TS. Therefore, to obtain a qualitative result of the state estimation (SE), the measurements used must be checked for the presence of distorted data. The SCADA data and SPM are processed in the SE problem, in which the power flow calculation is performed according to the measurement data [8,9].

The report considers the issues of applying the SE procedure for analyzing and improving the cyber-physical stability of the EPS and its facilities. It is shown that procedures detecting and compensating erroneous measurements serve as an effective means of identifying cyber attacks on SCADA and WAMS systems and eliminating their consequences, can significantly reduce the probability of distortion of the current state and improve the results of solving the tasks of dispatching control of the technological subsystem of the EPS.

2 Reliability and cyber-physical stability of Smart Grids

Security is one of the most important properties of an EPS, which ensures that the specified modes of the power system are maintained when operating conditions change, element failures and sudden disturbances. The problem of ensuring the security of electric power systems (EPS) is traditionally relevant for the electric power industry. Currently, a number of factors associated with the reform of the Russian electric power industry and the transition to market relations have led to

* Corresponding author: kolosok@isem.irk.ru

a decrease in the reliability and efficiency of the operation of the EPS.

To ensure a high level of system reliability and reliable power supply to consumers in normal modes of operation of the power system and to prevent emergency situations in a number of advanced countries of the world, including Russia, the process of building Smart Grids is underway. The use of the latest information technologies in the transition to Smart Grids creates new vulnerabilities in terms of cybersecurity, in this regard, deliberate intrusions or cyber attacks that threaten a large-scale power outage should also be considered as disturbances.

Existing approaches to the analysis of security relate mainly to the TS. Transitions from the normal state of a TS to an emergency state have been well studied by power engineers for many years [10,11, etc.].

At the same time, emergency conditions in the information and communication subsystem (ICS) due to failures and deliberate disturbances on its components can lead to a decrease in operational reliability and serious emergency conditions in the physical subsystem of the Smart Grids. Therefore, to analyze the stability of the Smart Grids and its objects to physical and information disturbances, i.e. Cyber-physical sustainability requires the development of new approaches to consider not only the technological, but also the information and communication subsystem, as well as their close relationship.

In a number of works [12-14], the reliability of the CPS of an electric power facility, consisting of two subsystems, is considered. The technological (physical) subsystem includes technical devices of primary equipment such as transformers, generators, reactors, bus coupler circuit-breakers, switches, disconnectors, relays, common auxiliaries, capacitor banks, etc., also includes electronic devices - PLC, IED, without which the operation of modern technical equipment is impossible. The ICS includes computing and network equipment, intelligent devices, software systems - everything that provides the collection, processing and transmission of information in digital form from physical components to the Control Center, as well as means of protection information.

As shown in [15] (Fig. 1), in the CPS, combined emergency conditions can occur, when a failure in the operation of one subsystem causes a failure in the second. The lack of electricity causes failure of the components of the information and communication subsystem (ICS) or the entire control unit, and vice versa, the erroneous results of the computing modules form incorrect control actions, causing, in turn, emergency events in the technological subsystem (TS).

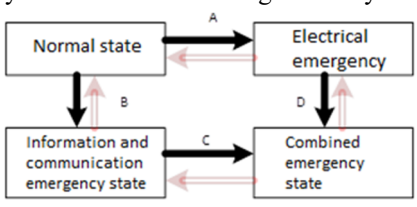

Fig. 1. States and transitions of the cyber-physical system [15].

One of the reasons leading to combined emergency events in the Smart Grids is malicious interference in its trouble-free operation. An analysis of events in the development of a number of systemic accidents in various countries, performed in domestic and foreign works, showed the presence of the mutual influence of failures and disturbances in the technological and information-communication subsystems of the EPS during the development of accidents (arrows of transitions to states C and D in Fig. 1). One of the main recommendations formulated in these works is the need to have a reliable and secure information and communication subsystem in the EPS that provides dispatch control tasks with information about the operating parameters obtained by estimating the state according to SCADA and WAMS data.

3 The role of the SE problem in providing the cyber-physical stability of the EPS

The organization of monitoring the state of the power facility in order to detect a sharp change in its state and subsequent response to this change will protect the power facility from making wrong decisions during management. For these purposes, programs are used that analyze operation parameters and can distinguish reliable information from false information and identify situations of malicious interference in the operation of power facilities. The category of such programs-analyzers includes software tools that implement the procedure Estimating the state of the EPS.

State estimation (SE) is a statistical data processing method used to check the reliability of data, filter measurement errors and recalculate unmeasured parameters. This task works on-line, detects the appearance of gross and systematic errors in the measurements of the operating parameters, identifies them and, if possible, determines the reasons for their occurrence. Locating the location of the error can help to find its source and cause.

The ESI SB RAS has developed a method of control equations for detecting erroneous data and assessing the state of the EPS [16]. The method was developed to detect incorrect data in SCADA measurements, then adapted to verify WAMS measurements and analyze the cybersecurity of data collection and processing systems - SCADA and WAMS - belonging to the information and communication infrastructure of the Smart Grid [17-18].

If deliberately false information comes from single recorders, then the SE task can independently cope with this problem, a priori detecting an erroneous measurement and replacing it with a pseudo-measurement. In the case when the attack is carried out on a large number of registrars, the number of erroneous measurements can lead to a divergence of the SE computational process. In such cases, the blocking of the SE task is provided, about which a message is issued to the dispatching personnel.

A large number of rejected measurements can lead to the loss of observability of the calculation scheme for the

SE. In this case, the SE is executed for the observed areas. In the unobserved part of the circuit, you can use the estimates from the previous cycle. One of the measures to combat the loss of SE observability is the installation of backup devices at power facilities for registering SPM, then when specific measurements are rejected, it will be possible to replace them with the values obtained from these backup PMUs.

To localize the impact site of a cyberattack, an SE algorithm was proposed in [19] based on the selection in the calculation scheme of areas observed by PMU. Performing a local SE for such areas separately according to SCADA and WAMS data, it is possible, based on the results of the SE, to determine which of these systems was attacked by a cyberattack.

In addition, the software itself, which implements the functions of the SE, can be subjected to cyberattacks. The main functions of the SE are the formation of the current settlement scheme according to TV signals; observability check; detection of gross errors in measurements and calculation of estimates of measured and non-measured parameters. In reliable SE software, all these functions should be duplicated [20].

Obviously, methods for detecting erroneous data and SE can give useful results in the event of emergency conditions in the information and communication subsystem and transitions from these states to the normal mode of the technological subsystem (transition B, shown in Fig. 1 by a red arrow). If the SE procedure cannot perform its functions due to disturbances in the ICS, then transitions to a combined emergency state occur (transition C, shown in Fig. 1 by a black arrow).

Based on the studies performed, Table 1 was compiled (with reference to Fig. 1.), which shows the possible transitions during the impact of a cyberattack on the ICS of a certain power facility and the functions that the SE procedure can provide to mitigate the consequences of such transitions.

Table 1. Interaction of cybernetic and physical subsystems of a power facility.

Transitions (Fig.1)	Information and communication subsystem (ICS)		Technological subsystem (TS)		The result of mutual influence
	Occasion	**Functions of the SE procedure**	**Occasion**	**State**	
B	Failure of the telemetry sensor or PMU	SE using additional pseudo-measurements	Regular mode	Regular mode	Both substations are functioning normally
	Failure of several telemetry sensors or PMU	Partial loss of observability. Distributed SE by monitored areas. Using estimates of the unobserved part of the scheme from the previous cycle.	Distributed SE by monitored areas. Using estimates of the unobserved part of the scheme from the previous cycle.	Regular mode	Both substations are functioning normally
	Cyber attack on SE software	Launch of duplicate algorithms of authentication blocks and SE.	Informing staff	Regular mode	Restoration of the OS program. TS in normal mode
	Cyber attack that led to a falsified break in the communication line	The division of the design scheme into subsystems, SE is performed using the decomposition algorithm	Regular mode	Regular mode	Both substations are functioning normally
	Cyber attack due to penetration into the local network, which did not lead to failures in the TS	Temporary shutdown of the ICS in the absence of a data protection tool	Regular mode	Regular mode	Recovery in the ICS. "Manual" control of the technologist / dispatcher in the work of TS is required
C	Complete non-receipt of SCADA and WAMS data	SE task in standby mode	The failure of the ICS led to the loss of information for the operator about the need for control action in the TS	Denial of TS	Recovery in the ICS, then in the TS Or "Manual" control action mode in TS
	Measurement out of sync	Incorrect results of calculations or divergence of SE computational process	SCADA and WAMS data are marked as FAILURE	Emergency mode	Requires "manual" control of the technologist / dispatcher at work TS Recovery in the ICS
	Cyber attack on SE task software (in the absence of	Failures in the computing process, emergency stop of the SE task	SCADA and WAMS data are marked as FAILURE	Emergency mode	Requires "manual" control of the technologist /

	duplicate SE algorithms)				dispatcher at work TS Recovery in the ICS
	Human factor	Making an incorrect decision on control action (contrary to SE results)	Dependent on staff	Deterioratio n in the TS	Recovery of a temporary failure of the TS. Troubleshooting by staff
	Penetration of a hacker into the ICP (theft or distortion of data, traffic overflow leading to failures in the TS)	Unable to run SE task	Dependent on external influence emergency event	Emergency state in TS	Independent recovery in each of the substations

As the obtained results showed, the application of the SE procedure to increase the cyber-physical stability of the Smart Grid and its objects requires a significant development and improvement of the methods and algorithms of the SE, which ensures the cybersecurity of the information and communication structure of the Smart Grid. As a development strategy, it is proposed to increase the redundancy of SCADA measurements, supplement them with WAMS measurements, to combine various methods for detecting erroneous data – a priori (Test equations method), a posteriori (analysis of evaluation residuals), robust criteria. Also it is proposed to use of criteria for the maximum probability of bad data detection when PMU is placed and to save the observability of the scheme when individual measuring devices failed.

4 Conclusion

In the process of “digitization”, both electric power systems and their objects acquire the properties of cyber-physical systems, in connection with this, the problem of ensuring the stability of the Smart Grid and its objects to physical and information disturbances or cyber-physical stability arises. The procedures for detecting and compensating for erroneous measurements in the EPS SE serve as effective means of identifying technical failures and intentional effects on information and communication subsystems and eliminating the consequences of failures on the results of solving dispatching control problems. This makes it possible to prevent the occurrence of complex combined emergency conditions and increase the reliability of the functioning of the cyber-physical system of the EPS and its objects.

However, as shown in [21], the transition from a "safe network" to a "stable network" requires the implementation of strategies to improve situational awareness of personnel for monitoring, forecasting, detecting and mitigating the consequences of extreme events, to increase network fault tolerance and develop tools and methods to detect emerging situations and correct them in a timely manner when minimal impact on the operation of the system. An important role here is assigned to the strategy of significant development and improvement of information collection systems and methods and algorithms for their processing.

This study was carried out within the framework of the state assignment project (No. FWEU-2021-0001) of the program of fundamental research of the Russian Federation for 2021-2030.

References

1. N.I. Voropai, Electrichestvo **7**, 12-21 (2020)
2. N.I. Voropai, I.N. Kolosok, E.S. Korkina, A.B.Osak, Energy Policy, **5,** 53-61 (2018)
3. B.V. Papkov, A.L. Kulikov, V.L. Osokin, Library of Electrical Engineering, **9**, 1-96 (2017)
4. D. Faquir, N. Chouliaras, V. Sofia, K. Olga, L. Maglaras, AIMS Electron. Electr, **5,** 24-37 (2021)
5. D. Westlund, *The Essential Role of Cyber Security in the Smart Grid*. Available: https://electricenergyonline.com/energy/magazine/312/article/ (accessed on 20 January 2023).
6. N.I. Voropai, I.N. Kolosok, E.S. Korkina, A.B.Osak, ESR, **3**, 19-28 (2020)
7. I.N. Kolosok, L.A. Gurina, *Information and mathematical technologies in science and management*, **2**, 40-51 (2019)
8. A.Z. Gamm, Yu.N. Kucherov, S.I. Palamarchuk et al, Nauka, *Methods of solving real-time problems in the electric power industry* (1991)
9. A. Abur A., A. G. Exposito, Marcel Dekker, Inc: New York-Bazel, *Power System State Estimation.Theory and Implementation* (2004)
10. N.I. Voropai, Nauka, *Reliability of power supply systems* (1991)
11. N.I. Voropai, Avtomatiz. IT Energet, **3**, 11 (2011)
12. D. Obychaiko, V. Shikhin, G. Chrysostomou, *Reliability Analysis of Cyber-Physical Systems*, in Proceedings of Intern. Conf. on Industrial Engineering, Applications and Manufacturing (ICIEAM), Moscow, Russia, 1-6 (2018)
13. B.V. Papkov B.V., P.V. Ilyushin, A.L. Kulikov, Scientific Publishing Center "XXI century", *Reliability and efficiency of modern power supply* (2021)
14. N.I. Voropai, I.N. Kolosok, E.S. Korkina, Relay protection and automation, **34**, 78-83 (2019)

15. A. F.D'yakov, V. A. Stennikov, S. M. Senderov et al, Nauka, *Reliability of energy systems: problems, models and methods of their solution* (2014)
16. A.Z. Gamm, I.N. Kolosok, Nauka, *Bad data detection in measurements in electric power systems* (2000)
17. E.S. Korkina. Abstract of the PhD Thesis, Development of methods for assessing the state of electric power systems based on the integration of SCADA and PMU data (2009)
18. A.M. Glazunova, I.N. Kolosok, *Solving problems of dispatching control of intelligent electric power systems on the basis of state assessment methods*, in Proceedings of Conf. "Power Engineering of Russia in the XXI century. Innovative Development and Management", Saint Petersburg, Russia, (2018)
19. I. N. Kolosok, E. S. Korkina, *Decomposition of power system state estimation problem as a method to tackle cyberattacks*, in Proceedings of the 1st IEEE Industrial Cyber-Physical Systems, ICPS, **58** (2018)
20. N.I. Voropai, I.N. Kolosok, E.S. Korkina, *Resilience assessment of the state estimation software under cyberattacks*, in Proceedings of E3S Web of Conferences (2018) DOI: https://doi.org/10.1051/e3sconf/20185802013
21. S. Basumallik, P. Chatterjee, *A. Grid resiliency against cyber threats and wildfires*, Available: https://energycentral.com/topics/tags/special-issue-2022-10-grid-reliability-resilience (accessed on 20 January 2023)