Preprints of the 21st IFAC World Congress (Virtual)
Berlin, Germany, July 12-17, 2020

Cyber security of electric networks with energy storages

I. Kolosok*, E. Korkina*, N. Tomin*

**Energy Systems Institute by L.A.Melentiev, Siberian Branch of Russian Academy of Sciences Russia (Tel: 7-395-2424700; e-mail: kolosok@isem.irk.ru, e-mail: korkina@isem.irk.ru)*

Abstract: Modern Energy Power Systems (EPS) are characterized by a rather high share of distributed generation, renewable energy sources (RES) and energy storage systems (ESS) operating under the control of smart devices. For transition to a qualitatively new level of power industry management, the developed countries create Smart Grids. An effect of sudden changes of loads, power flows in the lines, and changes in the generation, as well as other unexpected factors can negatively affect on stability and reliability of state of EPS as well as lower EPS flexibility that is one of the most relevant features of future energy systems. Use of ESS is one of the recognized options of maintaining the energy system flexibility. At the same time executing energy storages at an energy object and, moreover, their coordination using Internet-technologies globally increase cyber vulnerability of electrical network. At this paper different aspects of cyber security of electrical networks with energy storage units incorporated into them are shown and ways of their cyber resilience are considered. By arranging PMUs in power system nodes using ESS, awareness of the absence of cyber attacks can be increased.

Keywords: cyber security, energy storage system; PMU; Smart Grid.

1. INTRODUCTION

For transition to a qualitatively new level of power industry management, the developed countries create Smart Grids all the subjects of the electric energy market of which (power generation facilities, networks and power consumers) are active participants of power production, transmission and distribution. For raising the reliability, quality and economic efficiency of electric power, transition to Smart Grids (in area of generation) implies development and integration of renewable energy sources (RES), distributed generation and energy storages (ES) under control of modern intelligent devices, and their coordination using Internet-technologies.

Introduction of a larger number of RES and gradual transition from the centralized energy supply system to a distributed one lower the energy system stability and reliability, and, which is more important, its flexibility, which is one of the most relevant features of future energy systems. Flexibility is defined as ability of an energy system to keep and maintain normal operating conditions under the effect of internal (unexpected changes of loads, power flows in the links, and changes in the generation) and external (sudden disturbances) random (uncertain) factors (Cochran J. et al), (Haeger U. et al), (Zhao, J., et al.) Use of energy storages is one of the recognized options of maintaining the energy system flexibility. Ability of ES to accumulate electric energy and to output it at required time allows development of basically new approaches to optimum energy system management.

Despite obvious advantages granted by higher EPS flexibility, large-scale use of energy storages raises a number of problems. For a number of reasons one of problems of such networks is lower cyber resilience. They are exchange of data and commands with an energy consumer and a control center via opened communication channels and Internet protocols, use of cloud computing, mobile applications, and interaction with Industrial Internet of Things (IIoT), etc. that increase the number of potentially vulnerable places in the network (Wang, Z. et al). Thus, all factors above require a careful study of the problem of cyber security of electric networks with energy storages.

The paper consists of six sections. Section 2 gives brief description of types of energy storages, ways of their integration into the energy supply system, and peculiarities of ES aggregation when an energy storage system participates in the electric energy market. Section 3 is devoted to the problems of ES cyber resilience, to cyber threats faced when energy storages are in-built into a distributed structure of an electric energy demand Aggregator. Section 4 offers ways for increasing the resilience of networks with ESs. In Section 5 there are our approach to such cyber security decision concluding in PMU installation at network areas with ESSs. Section 6 summarizes the problems considered.

2. ENERGY STORAGE DEVICES AND SYSTEMS

The trend of today is the development of technology and the production of energy storage systems. New types of energy storages, such as electrochemical storage batteries, rotor-type storage devices, compressed air electric storage devices,

This study is supported by grant № 19-49-04108. "Development of Innovative Technologies and Tools for Flexibility Assessment and Enhancement of Future Power Systems".

Copyright lies with the authors

superconductor-type storage units, and super condensers have been used for power storage lately.

The fundamental difference between the ESS and traditional uninterruptible power supplies is that the energy storage system is connected not in series between the network and the load, but in parallel with the network. This allows, in addition to the uninterruptible power supply function, to implement a number of useful functions. ESS, in fact, has two key capabilities: the consumption of electricity from a generator (or network) and the return of electricity to a load or network.

Depending on their purpose and location, ESS can be connected to the network in different ways: 1) on the side of a large energy or grid complex in parallel with a centralized power supply network; 2) in a block with renewable energy sources (solar panels, wind turbines) in remote and isolated areas; 3) at the consumer level in the architecture of the Aggregator of distributed energy resources (DER).

There are three Models of using ESS in the energy system:

1. A model of using large "network" ES directly in the centralized power supply network at the level of power generation and/or transmission;
2. A model of using separate large- and mid-size ES within a micro network of an industrial enterprise or within a small independent energy system;
3. A model of consolidation and joint management of a large number of distributed ES ("a virtual energy storage facility").

Energy storages are the most important component of developing Smart Grids as they ensure (Kulikov Yu.):

- Leveling the load curves in a network owing to electric energy accumulation in the period of excessive (cheap) power, and its supply to the network in the periods of power shortage;
- Participation in frequency control (primary and secondary control);
- Integration of RES into the energy system;
- Continuous power supply for facilities of major importance, for auxiliary needs of power plants, substations, etc.

3. CYBER VULNERABILITY OF ENERGY STORAGES

In Russia due to the incompleteness of the regulatory framework for the inclusion of energy storages systems in the energy supply system (The concept of the functioning of aggregators…) ESSs aren't rated as either generation or the consumer of energy power, at the moment they are a category of system services. Energy storage systems can be considered as sources of critical information for an EPS, as along with their functions proper they are involved in the information-communication system that is subjected to ill-intentioned attacks. Thus, ESS needs cyber protection. Let us consider each Model of integrating ESS into Energy Supply System from the standpoint of cyber vulnerability and consequences for EPS operation.

In Models 1 and 2 the problems related to cyber security of ESS management system do not basically differ from similar problems related to generating capacities management (though there may be some peculiarities due to specific modes of ES operation).

Model 3 implying aggregation of a large number of distributed ESSs and demand management is the most perspective one, though it is most vulnerable from the standpoint of cyber security.

3.1 Model 1. ESS operation in parallel with network. Model2. ES installation and operation in an independent power supply system in the RES block or at the level of a consumer

Let us consider ESS installed on a large industrial object. According to (Potapenko A., and Melnikov V), system of ESs consists of the following subsystems:

- A management subsystem supports monitoring and communication with the automatic process control system (APCS) of a higher level;
- A subsystem of conversions converts energy from a DC link (storage) to an AC link and back following the control system command.
- An energy storage subsystem. Elements charging and monitoring of their condition are controlled with a Battery Management System.
- A distribution subsystem. It includes switching devices, coordinating transformers and relay protection devices.

ESS is a kind of cyber-physical structure (CPS), which consists of physical subsystem (bi-directional inverter, charging elements, transformers and relay protection devices) and of information subsystem (management subsystem, BMS). In any CPS, damage to one of the subsystems leads to a malfunction of the other subsystem. From the point of view of cybersecurity, vulnerable components of ESS are (https://e-solarpower.ru), (https://www.cyberpower.com/...):

- BMS electronic board, as the firmware of the board may be unreliable, which will lead to poor-quality operation of the inverter;
- wired and wireless communications, which transfer data from BMS to external devices. The distortion of this information will cause a malfunction in the operation mode of mobile devices to manage the reduction of energy consumption during peak loads;
- SCADA systems and process control systems external to ESS, which are also vulnerable to cyber attacks. The distortion that came from external systems will damage the correct operation of the ESS control subsystem and lead to a violation of the sequence, duration and speed of battery charging / discharging processes and other types of energy storages.

Figures 1, 2 show cyber-vulnerable spots of a scheme with integrated energy storage. Bold (red) two-directional arrows show the ways of possible distribution of cyber attacks.

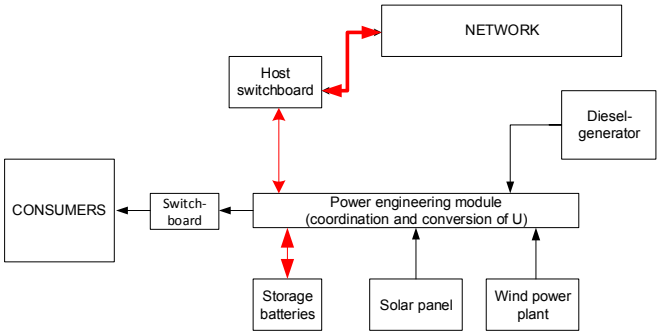

Fig. 1. Cyber vulnerability of an energy storage working in parallel with the network.

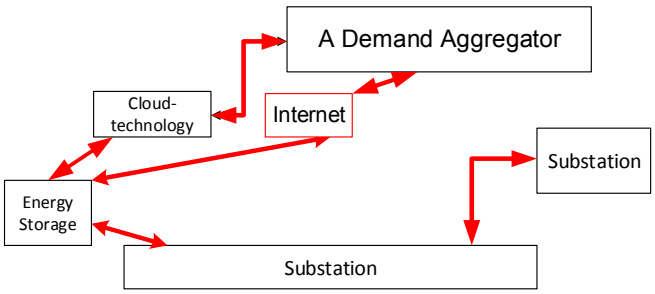

Fig. 2. Cyber vulnerability of an energy storage system within the distributed Aggregator's system.

3.2 Model 3. ESS as an element of the electricity market. Aggregators of Distributed Energy Resources (DER)

A Concept of Energy Resources Market Aggregators Operation within the Interconnected Energy System (The concept of the functioning of aggregators…) has been developed in Russia that provides for implementation of pilot projects in 2019-2020 within which Aggregators will be working at the market of services on ensuring the systems reliability.

A Demand Aggregator is a structure (power sale companies, networks, independent players of the electric energy market) capable to manage consumption modes of equipment of a large number of retail customers. Aggregator's objective is involvement of retail consumers ready to reduce their consumption against Systems Operator's command in order to lower peak consumption and reduce energy system's expenses on peak generation. Demand Aggregators make the system more flexible and efficient thus making the electric energy cheaper. Moreover, Aggregators have technical capabilities for physical connection of consumers and for uniting their loads into a single cluster that can be territorially distributed and remotely controlled via Internet and 'cloud' technologies. This activity implies availability of a complex communication infrastructure and a centralized IT system capable to ensure control over a large set of loads with different characteristics.

IIoT application in power engineering (IoEN) (Market for energy storage systems…) would raise the efficiency of electric power production and distribution, including in the area of applying the distributed generation and energy storages. Data on distributed facilities in this case are transmitted to the 'cloud' for storage and interpretation, where a network dispatcher 'sees' them and can use them for making control commands. At the same time, data transmitted between IIoT devices are rather vulnerable from the standpoint of security. The main security threats in a cloud include(Threats to cloud computations…): theft and losses of data; crack of accounts; loopholes in the interfaces and in Application Programming Interface (API); DoS-attacks; activities of insiders; penetration of hackers; and idle time through provider 's fault.

Wide application of 'cloud' computations, mobile apps and interaction with Internet of Things would raise the number of potentially vulnerable places.

4. MEASURES AIMED AT RAISING THE RESILIENCE OF NETWORKS WITH ENERGY STORAGES

In case of a successful cyber attack the situation occurs when it is impossible to timely transmit a managerial command to startup ES, irrespective of the method of ESS integration into the energy system (independent, parallel with the network, or distributed one). Therefore, it is necessary to enforce measures ensuring the cyber resilience of the Smart Grid section where ES (of any type) is installed.

4.1 Model 1. Raising the resilience of ESS operation in parallel with network. Model 2. Raising the resilience of ESS in an independent power supply system in the RES block or at the level of a consumer

Cyber-resilience of networks with ESS working in parallel can be raised in two ways:

- Protection of ESS proper working in parallel with the network;
- Development of measures for raising the resilience at a level of the network.

Protection of an energy storage system operated in parallel with the network shall be organized for all the subsystems, starting from Automatic Process Control System (APCS) with an in-built system for ESS management, and downwards to the level of controllers. For enhancing the overall security level, the main measures for raising the resilience of such ESS have been identified:

- Disconnection of APCS from Internet and use of intricate passwords (In Russia 591 components …);
- Earthing the sources of electromagnetic radiation (PC, active elements of local networks and cables), shielding the rooms, use of special completely radio-isolated computers, etc. (Hardware used for data processing...);
- Automatic updating of antivirus software (Energy specialists on Win32/Industroyer…), (Protection of devices against chip-related security vulnerability…);
- Coding the communication between PC and a facility (public key systems)) (Demina);

- Disconnection of USB-ports in case of computer's screen blocking (Ivanov);
- Protection of a controller whose failure may interrupt the facility operation or operation of a block of management system objects (Protection of a device from cracking and ...), (AVR. Training course.).

Raising the resilience of networks with ESF operated at the level of a network has much in common with such important feature as mode reliability and survivability that ensure normal EPS operation (Voropai, 1991). In the present-day conditions of transition to intelligent energy systems, digitalization of energy industry, high vulnerability of intelligent energy systems on the whole and of their infrastructure components towards cyber attacks, these fundamental features are complemented by resilience property, i.e., ability of sophisticated technical or informational systems to survive and maintain their availability in the conditions of cyber attacks. Despite seeming novelty of this property, methods for its support are in many ways similar to those developed and applied for ensuring the reliability and survivability of EPS (Reliability of energy systems…), (Voropai et al, 2018). They include: optimum allocation of ES, backup, ensuring power margins, etc. with account of peculiarities and tasks whose solution require some or other ES. Cyber attacks may lead to partial or complete failure of ES, to errors in networks management up to heavy blackouts, to reduction of EPS efficiency and operability. For this reason ES shall be allocated with account of the following main criteria (Stroev et al):

- Minimization of the number and period of interruptions in power supply for consumers in case of different emergencies;
- Minimization of the scope of electric equipment (transformers, transmission lines) that requires replacement due to current overload in emergency;
- Minimization of losses in the electric network owing to leveling the load schedule and maintaining the voltage in the nodes of a loop;
- Economically efficient management of power consumption and power supply modes of ES with account of different tariffs for different periods of a day.

4.2 Model 3. Raising the resilience of ESS in Aggregators of Distributed Energy Resources

In this Model the problems related to application of IoEN technology and 'cloud' computations (Volkov), (Young) for communication of an independent ESs with the Aggregator and/or dispatching control center become top priority ones. They require warranty of failure-free operation and reliable power supply of DPC, which necessitates organization of both network and physical security. Physical security implies severe control over physical access to servers and network infrastructure. Network security is primarily development of a reliable model of threats that includes protection from attacks and an inter-network screen. A system of attacks detection and prevention shall be capable to detect an ill-intentional activity at the level of virtual machines irrespective of their location in the cloud medium.

In the development of the Russian Pilot Project of the Aggregator of DER, the authors of (RTSoft forms…) applied the protection of On-premise cloud technology - the creation of specific clouds of increased security with a limited number of users. If the exchange of information takes place over a protected cloud, then the management of the ESS itself remains unprotected. In this case, the end consumer experiences cyber threats to energy storage devices, since on its side of the network there are vulnerable network connections (wired, wireless, mobile), vulnerable industrial Modbus protocols designed for operation of drive controllers, smart meters through which ESS and RES are combined, but not having cyber defense. In addition, there is a cyber threat of network penetration through gadgets, where software is installed and launched to control the reduction of consumer power. Thus, the issue of cyber resistance of ESs and ESS management software should be addressed locally at the consumer level, taking into account their technical capabilities.

The present paper offers a Hybrid Tree of Threats and Attacks for visual imaging of:

- places vulnerable to functionality threats to a physical element (a subsystem), and
- for localization of undertaken cyber attacks and their consequences (damages, destruction) for those elements (subsystems).

Superposition of a Tree of Threats and a Tree of Attacks in one figure gives more thorough understanding of the threats to Energy Storage Systems and allows elaboration of measures for their protection from Cyber Attacks. It should be kept in mind that vulnerabilities throughout the tree shall be considered in complex, i.e., from the tree root downwards to the level of an undertaken Cyber Attack.

For illustration of Cyber Resilience of ESS, an approach to solution of Demand Response (DR) problem within Russian Pilot Project has been offered: members of this Project take an obligation to reduce power consumption for four hours a day several times a month. The DR problem can be considered within Power quality & reliability or Peak shaving options. Each member can solve the DR problem on reduction of power consumption in his own way:

- They may shift daily load to the period of the day with lower power prices;
- They may compensate a part of power undersupplied by Energy Supply Systems by power supplied by Energy Storage Systems;
- They may temporarily shut down some units or disconnect some consumers, etc.

But these options require clarification of the following key issues: What types of ESS shall be used? Which routine technological problems shall be solved by participants with the help of Energy Storage Systems during the Pilot Project? Do they take into account probability of equipment failure during participation in the Project?

Fig. 3 shows the details of Threats and Attacks Tree during solving the DR problem using the Demand Aggregator. Each cluster includes generation (G), load (L) and energy storages (ES).

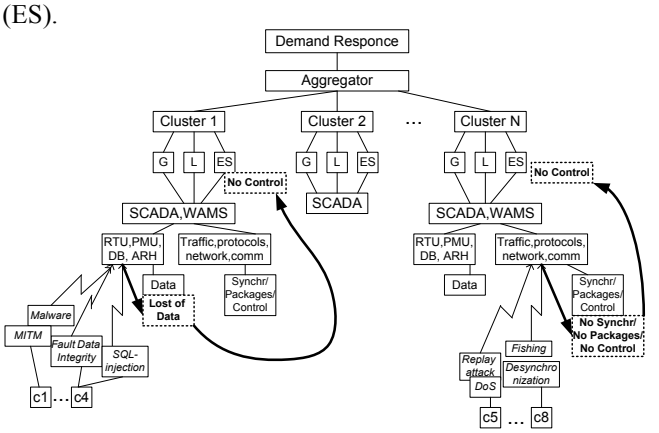

Fig. 3. A Hybrid Tree of Threats and Attacks

Measured data in the network are acquired and transmitted using SCADA and WAMS systems. Despite observing all the security requirements, the data acquisition system, nevertheless, has many vulnerable places, namely, RTU, PMU, etc., databases (DB), and archives (ARH). All the on-line and reference information is under threat. In case of a cyber attack aimed at counterfeiting or theft of data, the DATA will be LOST as a consequence of a Cyber Attack (see Cluster 1), which would cause incorrect calculation of current mode and improper Energy Storage System control. There may also be Cyber attacks causing network-related problems, i.e., penetration into the network, malicious attacks inside the networks, and distortion of data package routes. Such attacks would result in heavy consequences, such as traffic overflow, loss of data packages, loss of synchronizations, etc., (see Cluster N) to be unavoidably followed by loss of Energy Storage System control.

Any Tree of Attack at its lower level contains a list of countermeasures (c1, ... cN) for protection of any branch of a Tree from Cyber Attacks. The more statistical data on some or other Cyber Attack is available, the larger the amount of countermeasures developed. Examples of countermeasures are given in Section 4.

5. USE OF THE PMU INSTALLATION FOR WARNING CYBER ATTACKS IN NETWORKS WITH ESSs

In our opinion, increasing consumer awareness of the absence of cyber threats can be organized with the help of PMU arrangement, high-precision time-synchronized devices for measuring electrical quantities. To date, approaches to installing PMU are well developed to solve the problems of the EPS state estimation , forecasting energy consumption and other problems of EPS operational control (Abur, Exposito), (Gamm et al).

In (Wang, S. et al), (Bhattarai et al), aggregator clustering models were proposed. The consolidation of end-users of the distribution network level into clusters can be considered as a kind of decomposition problem. Approaches to the PMU placement for the decomposition problem in EPS dispatch control are worked out (Abur, Zhao, L.), (Kolosok et al, 2011). The main conditions for solving the decomposition of a power system into subsystems are conditions for equal voltage at the boundary nodes of neighboring power systems or a balance of power flows in the boundary lines. In this case, all nodes of the original network must fully enter the subsystems.

Aggregators of DER include only those nodes that can be joined according to one of the properties (by territorial sign, by type of load, by type of demand management model, by thermostatic characteristics). A prerequisite for the correct operation of the Aggregator is to maintain the balance of import and export of energy power in this cluster.

In connection with increasing cyber threats in the energy sector, studies are also underway to use PMU measurements to detect cyber attacks (Yang et al), (Kolosok, Korkina).

Combining the problems of decomposition and cyber security into a common problem, we propose placing PMUs in aggregator nodes and consumer nodes to provide gathering phasor data of nodal voltages. Such information will allow us to analyze the voltage levels, frequency, magnitude of the consumed load and the generation volume in the aggregation region under consideration. Sudden changes in the incoming measurements, which are not provided for by the basic graphs of decreasing and increasing the load, will be interpreted as signals of intrusion into the information subsystem of the network with ESS.

6. CONCLUSIONS

Cyber resilience of ESS is a kind of warranty of reliable operation of an energy facility. But it should be taken into account the energy storage systems can be integrated into energy supply systems in different ways.

When ESS is operated in parallel with energy supply systems, it is included into a local network of an energy facility that is vulnerable towards cyber attacks through network elements, data exchange protocols, overloaded traffic, and through other possibly vulnerable factors of an information-communication system.

In case of independent ESS operation it can be involved into Aggregator's energy consumption facilities and become a component of a distributed management system that uses Internet networks and cloud technologies, thus creating even a more vulnerable to cyber-attacks structure.

For raising the ESS resilience, prior to its integration into the network, all the possible vulnerabilities of an information and communication system of the facility shall be thoroughly analyzed; options of its participation or failure to participate in the Aggregator's power consumption facility shall be investigated; approaches to administer the access rights, and other organizational issues shall be well thought over.

Increasing consumer awareness of the absence of cyber threats can be organized with the help of PMU arrangement, high-precision time-synchronized devices for measuring electrical quantities. Sudden changes in the incoming

measurements, which are not provided for by the basic graphs of decreasing and increasing the load, will be interpreted as signals of intrusion into the information subsystem of the network with ESS.

REFERENCES

Abur, A., and Exposito, A.G. Power System State Estimation – Theory and Implementation. New York: Marchel Dekker, 2004.

Abur, A., and Zhao, L. (2005). Multiarea State Estimation Using Synchronized Phasor Measurements. IEEE Transactions on Power Systems 20(2): pp.611–617.

AVR. Training course. Use of Bootloader. http://easyelectronics.ru/avr-uchebnyj-kurs-ispolzovanie-bootloadera.html

Bhattarai, B.P., Mendaza, I.D.de Cerio, Myers, K.S., Bak-Jensen, B., and Paudyal, S. (2017). Optimum aggregation and control of spatially distributed flexible resources in Smart Grid.

Cochran J., Miller M., Zinaman O., Milligan M., et.al. (2014). Flexibility in 21st Century power systems // 21st Century Power Partnership, Denver,USA, Clean Energy Ministerial, pp. 1-14.

Demina K. Controllers are control devices in electronics and computer hardware. Controller: Definition, diagram, design and types. https://www.syl.ru/article/372726/

Energy specialists on Win32/Industroyer: no need to push the panic button (2017). http://digitalsubstation.com/blog/2017/06/28/energetiki-o-win32-industroyer-panikovat-ne-stoit/

Gamm, A., Grishin, Y., Glazunova, A., Kolosok, I., Korkina, E. (2007). "New EPS state estimation algorithms based on the technique of test equations and PMU measurements", "PowerTech".

Haeger U., Rehtanz Ch., and Voropai N. (2012). ICOEUR project results on improving observability and flexibility of large-scale transmission systems // IEEE PES General Meeting, San Diego, USA, 7 p.

Hardware used for data processing. https://studfiles.net/preview/5866837/page:4/

https://e-solarpower.ru/faq/sistema-upravleniya-batarei-bms/

https://www.cyberpower.com/ru/ru/product/series/battery_management_system

In Russia 591 components of Automatic Process Control Systems are available through Internet (2017). http://digitalsubstation.com/blog/2017/05/16/v-rossii-cherez-internet-dostupen-591-komponent-asu-tp/

Ivanov, O. Main vulnerabilities in USB security. https://www.anti-malware.ru/analytics/Threats_Analysis/security-flaws-in-usb

Kolosok, I., and Korkina, E. (2018). Decomposition of Power System State Estimation Problem as a Method to Tackle Cyberattacks 1st IEEE Industrial Cyber-Physical Systems, ICPS. DOI: 10.1109/ICPHYS.2018.8387691

Kolosok, I., Korkina, E., and Paltsev, A. (2011). Bad Data Detection at Decomposition of State Estimation Problem. "PowerTech', Trondhaim, Norway. doi:10.1109/ptc.2011.6019459

Kulikov Yu. A. Electric energy storage facilities as an efficient tool for managing the operating conditions of electric power systems. http://www.fondsmena.ru/media/EGM_publicationfiles

Market for energy storage systems in Russia: development potential. Edited by Yu. Udaltsov and D. Holkin.(2018). Moscow, center for strategic development,

Potapenko A., and Melnikov V. Energy storage facilities in the electric power supply systems of industrial companies. http://estorsys.ru/publications/sistemy-nakopleniya-energii-v-sistemah

Protection of a device from cracking and downloading. http://we.easyelectronics.ru/blog/Soft/2570.html#BoardProtection

Protection of devices against chip-related security vulnerability https://support.microsoft.com/ru-kz/help/4073229/windows-protect-device-against-chip-related-security-vulnerability

Reliability of energy systems: Problems, models and methods of their solution / Diakov, A., Stennikov, V., Senderov, S., Sukharev M. et al.; (2014). Editor N. Voropai. Novosibirsk: Nauka, – 284p.

RTSoft forms the community of the Russian software platform for distributed power engineering management. (2018). http://www.rtsoft.ru/press/r1/rtsoft-formiruet-soobshchestvo-rossiyskoy-programmnoy-platformy-dlya-upravleniya-raspredelyennoy-ene/

Stroev, V., Gremiakov, A., Arachchige, C., and Styczynski, Z. (1999). Optimal Allocation of Energy Storage devices in electrical power systems. 13-th PSCC in Trondheim, pp.510-515.

The concept of the functioning of aggregators of distributed energy resources as part of the Unified Energy System of Russia (2017) https://www.so-ups.ru/fileadmin/files/company/markets/dr/docs/dr_aggregator_concept.pdf

Threats to could computations and methods of their protection. https://habr.com/ru/post/183168/

Volkov V.A. (2015). Analysis of threats and methods of protecting cloud services. «Young Scientist», № 12 (27), pp.38-43.

Voropai N. (1991). EPS Survivability: Methodological grounds and methods of studies // Izv. AN SSSR. Energy and transport, № 6, p. 52-59.

Voropai N.., Kolosok I., Korkina E., and Osak A. Problems of vulnerability and survivability of cyber-physical and electric power systems // Energy Policy, № 5, 2018, pp.53-61

Yang, G., Gordon, M., Nielsen, A.H., and Østergaard, J. (2009). PMU Applications - From Situation Awareness to Blackout Prevention. DTU–Siemens, Future Energy Systems Workshop. orbit.dtu.dk

Young, M. (1989). The Technical Writer's Handbook. Mill Valley, CA: University Science.

Zhao, J., Zheng, T., and Litvinov, E. (2016). A unified framework for defining and measuring flexibility in power system // IEEE Trans. Power Syst., 31(1), pp.339-347.

Wang, S., Xue, X., and Yan, C. (2014). Building power demand response methods toward smart grid. DOI: 10.1080/10789669.2014.929887

Wang, Z., Nistor, M.S., and Pickl, S.W. (2017). Analysis of the definitions of resilience // The 20th IFAC World Congress, Toulouse, France, pp.11136-11144