Intelligent Control and Protection of Power Systems in the Russian Cities

Nikolai Voropai, Victor Kurbatsky, Nikita Tomin, Dmitry Efimov and Irina Kolosok
Electric Power System Department, Melentiev Energy Systems Institute, Irkutsk, Russia

Keywords: Power Grid, Smart Cities, Control, Protection, Artificial Intelligence, Russia.

Abstract: A distinctive feature of the energy system development in Russian megalopolises is the need for a comprehensive approach to the problem of making the network intelligent. The paper presents the following contributions: (1) intelligent operation and smart emergency protection in Russia including requirements for new protection systems; (2) a description of smart grid territorial clusters in the interconnected power systems of Russia. (3) state estimation (SE) techniques as informational support of the intelligent power grid control including SE with phasor measurements use, dynamic SE, and cyber-physical security issues of SE; (4) a hybrid Volt/VAr control approach based on AI techniques such as machine learning and multi-agent systems based models.

1 INTRODUCTION

Cities today are home to more than 50 percent of the world's population and by 2050 it is estimated that 2.9 billion people will be living in cities. These cities and megapolosies will need new and intelligent infrastructure to meet the needs of their citizens and businesses (ABB, 2013).

Cities might experience significant concentrations of electric vehicles and renewables in certain city districts. Left unmanaged, new loads can dramatically increase load on the system at certain times of the day and cause circuit breakers or fuses to trip with resulting outages. The traditional response would be to resize substations or strengthen distribution lines and equipment. Grid automation can be used to defer some of these upgrades.

While city grids are generally strong enough to integrate renewables without significant capacity or voltage challenges, additional power system protection is required to cope with bi-directional fault currents. With distributed renewables, at certain times renewable generation could exceed consumption, resulting in power flowing from the customer into the grid. New protection schemes are required to cope with these situations safely and isolate only those parts of the grids experiencing problems.

Large cities and megalopolises of Russia (Moscow, St.-Petersburg, Yekaterinburg, etc.) represent the most dynamically developing territories of Russia with a growing electricity demand after the economic crisis of 1998. These territories require special attention when planning the development of energy infrastructure and have a number of characteristic features. In the nearest future the development of the networks in megalopolises and large industrial centers in Russia will result in the formation of systems with a complex multi-loop structure (Voropai, 2016).

A distinctive feature of the energy system development in Russian megalopolises is the need for a comprehensive approach to the problem of making the network intelligent. It is reasonable to consider the entire process of production, transmission, distribution and consumption as a single whole rather than divide the processes according to the balance inventory as this has been done lately. Accordingly, a staged introduction of automated control based on the intelligent principles will improve the reliability of the entire power system operation. Furthermore, it will increase the quality of electricity supply to consumers.

An effective way to support these city goals is by using technology to more intelligently monitor, optimize and control key systems and infrastructure. In other words, to operate as a 'smart city'.

The evolution of the traditional electrical system in the direction of the intelligent grid implies a growing automation of the power grid management

Voropai, N., Kurbatsky, V., Tomin, N., Efimov, D. and Kolosok, I.
Intelligent Control and Protection of Power Systems in the Russian Cities.
DOI: 10.5220/0007656700190029
In *Proceedings of the 8th International Conference on Smart Cities and Green ICT Systems (SMARTGREENS 2019)*, pages 19-29
ISBN: 978-989-758-373-5

in order to increase operating efficiency, increase reliability, expand the use of network assets, reduce emergencies, etc. To achieve these objectives in 2014, President of the Russian Federation Putin V.V. was announced one of the nine road maps of the National Technology Initiative "EnergyNet", which is a high-level long-term program for the development of technologies, standards and communities in the field of building the electric power industry for the new technological structure.

Integration of power systems, liberalization, and modernization of the electric power industry increase the changeability and unpredictability of electric power systems operation and generate the need to improve and develop principles as well as systems of operation and emergency control. Artificial intelligence application is an advanced way to carry out smart emergency control in power systems (Efimov, 2011; Voropai, 2011; Voropai, 2018).

2 SMART GRID CLUSTERS IN RUSSIA

The process of intelligent power system formation under the EnergyNet platform suggests pilot projects implementation and territorial smart grid clusters creation. These clusters are supposed to use information, technological, and control systems providing adaptive control of network parameters, remote control of switching devices, and real-time estimation of the network technical state under normal, pre-emergency, and post-emergency conditions (Efimov, 2011; Efimov, 2012).

Currently, along with implementation of the pilot projects and the creation of smart grid clusters, new equipment is being installed at the energy facilities of the unified national electric grid of Russia as a part of a modernization program. In Russia the projects on formation of individual smart grid clusters and implementation of pilot projects aimed at creating the smart grid were launched in 2011 (Efimov, 2011; Voropai, 2011; Budargin, 2010).

Below we briefly indicate several most important pilot projects, which are implementing in two (of the seven) interconnected power systems belonging to the unified energy system of Russia.

The following pilot projects of smart grid clusters will be implemented in the north-western region of Russia during the period through 2020 (Fortov, 2012; Efimov, 2011; Efimov, 2012; Budargin, 2011): Karelskaya power system, power systems of Komi Republic and Arkhangelsk city, and "Big Ring" and "Small Ring" of electric networks in St. Petersburg (Table 1).

Table 1: Pilot projects on creation of territorial clusters of the smart grid in the Northwest interconnected power system.

Smart grid cluster	Project goal
1. KOLA (Karelskaya power system)	To provide reliable power supply and power quality under conditions of parallel operation of 330 kV transit overhead transmission lines
2. KOMI (power system of Komi Republic and Arkhangelsk power system)	To provide high reliability level of power supply at the required power quality
3. BIG RING (St. Petersburg)	To ensure required reliability of power supply to urban consumers
4. SMALL RING (St. Petersburg)	To decrease current loading and redundancy of existing lines

Table 2: Pilot projects on creation of territorial clusters of the smart grid in the East interconnected power system.

Smart grid cluster	Project goal(s)
1. ELGAUGOL	– To provide power quality and redundancy of tunneling and traction power supply (a two-circuit 220 kV transit transmission line) – To ensure emergency and operation control, considering development of small-scale generation
2. NIZHNY KURANAKH-MAIYA (Yakutian power system)	To provide a high level of power supply reliability and power quality
3. VANINO	To increase the reliability of the power supply to traction substations of the electrified railway in the Khabarovsk Territory
4. PRIMORYE TERRITORY	– To supply electricity to the southern part of the Primorye Territory – To increase transfer capabilities of 500 kV transit transmission lines by 350–400 MW
5. RUSSKY & POPOV ISLANDS with distributed generation	– To integrate wind generation and mini-CPP into the grid – To provide power quality and redundancy – To ensure emergency and operation control, considering small-scale generation expansion and involvement of storage devices

The pilot projects are intended to furnish Northwest interconnected power system with innovation technologies of smart grids that will effectively solve the regional problems (limitations on power output from power plants, insufficient reliability level of power supply to consumers, etc.).

Table 2 presents pilot projects in the territory covered by the East interconnected power system of Russia (Amur region, Sakha Republic, Primorye, and Khabarovsk Territories). The projects address to electric power networks of megalopolises and include several smart grid clusters.

Implementation of smart grid in the clusters "ElgaUgol", "Vanino", and "Primorye Territory" suggests construction of compact digital substations furnished with innovative devices (new systems for reactive power compensation and voltage maintenance, active filters, equipment monitoring and diagnosis systems, etc.)

The territorial smart grid cluster was formed at Russky Island (Efimov, 2011; Voropai, 2011; R&D Report, 2009). It involves the creation of a smart automated control system, which aims to provide centralized monitoring, dispatching, and process control as well as solving the problems of creating the smart grid of the region and optimal control of electricity, heat, and gas supply facilities and consumers. Alongside the network infrastructure, the integrated smart grid includes gas-fired power plants (mini-CHPPs), wind farms, boiler plants, electricity and heat storage systems, "smart houses," and a park of electric vehicles with charging stations.

3 INTELLIGENT EMERGENCY CONTROL AND REQUIREMENTS TO LOAD SHEDDING ALGORITHMS

Emergency control philosophy in the unified energy system of Russia is a hierarchical approach and is realized by the coordinated operation of many control devices, which maintain power system stability and interrupt the expansion of an emergency situation in the case of stability violation and a threat of undesirable cascade emergency development. Coordinated emergency control is realized by joint participation of generators, networks, and consumers. Such approach can be also realized for emergency control of large cities and megalopolises based on smart grid technologies and ideology of EnergyNet platform.

The components of emergency control system are shown in Table 3.

Table 3: Emergency operation control services.

Conditions	Services	Aims
Pre-emergency	- Emergency dispatching - Transfer capability control	- To maintain transfer capability margins of transmission lines - To increase transfer capabilities of ties by voltage control
Emergency	Emergency control	- To provide EPS stability by increasing voltages and damping the oscillations - To provide EPS stability by automatic stability control - To interrupt emergency development by automatic devices
Post-emergency	Restoration	To provide fast EPS restoration by observing the margins and excluding restoration disruption

Table 4: Functions and types of emergency control automations.

Functions of the emergency control automations	Main types of emergency control systems
Centralized hierarchical automation	
Prevention of stability violation (this is the function of centralized automatic stability control system)	*Automatic Stability Control System* is arranged according to the hierarchical principle with the levels of: – the UES of Russia – a coordinating emergency control system; – interconnected or regional power system – centralized emergency control systems; – power industry facilities – local automatic systems.
Standalone (local) automations	
Elimination of out-of-step conditions	*Out-of-Step Protection System*
Limitation of frequency decrease or increase	*Automatic Underfrequency Protection*, including: – automatic load transfer, – automatic frequency load shedding (three types, several stages), – additional load shedding, – under/over frequency islanding, – frequency actuated automatic reclosing
	Automatic Overfrequency Protection
Limitation of voltage decrease or increase	*Automatic Undervoltage Protection*
	Automatic Overvoltage Protection (two stages)
Prevention of inadmissible overloads	*Automatic Equipment Overload Control* (several stages)

According to Russian standards (National Standard, 2012; National Standard, 2013), the emergency control systems and devices are intended for the detection of emergency conditions in energy system, prevention of their development, and elimination. The most important task of the emergency control systems is prevention of system-wide blackouts accompanied by an interruption in electricity supply to consumers in a large territory. Hence the main functions of emergency control and corresponding types of the emergency control automations may be classified as in Table 4.

Most of the difficulties in power system operation are caused by electrical grid overloads. Load shedding in the receiving subsystem is the most efficient action among the remedies against overload. Basing on those considerations the principles and algorithms of distributed adaptive load shedding against stability loss of the ties of main network and overcurrents of controlled subsystem lines are to be developed.

A new load shedding scheme was proposed in (Voropai, 2018) as a combination of disconnections either large or small consumers – it means disaggregation and distribution of load shedding automation (Fig.1).

From technical point of view, the easiest way of emergency load shedding is a piecemeal disconnection of large industrial consumers, which are connected with the power system in high voltages, see Fig.1(b). It is the usual present practice. At the same time, the economic damages caused by such kind of disconnections can be considerable (for example, the loss of profit due to technological cycle interruption). The compensation of the potential damages (for example, with preferential prices of electricity for consumers, which agree to emergency limitation of electricity supply) could be very unprofitable for power system.

Coming from these considerations an alternate load shedding scheme can be proposed as a combination of disconnections either large or small consumers – it means disaggregation and distribution of load shedding automation, see Fig.1(c). It is more difficult technically than disconnection of large consumers, but present state of automation and data transmission systems makes it feasible. The advantages of small loads emergency disconnections are much smaller total damage, and ability of more accurate dosing the disconnections (if the large consumers are disconnected then the surplus load disconnection is practically imminent).

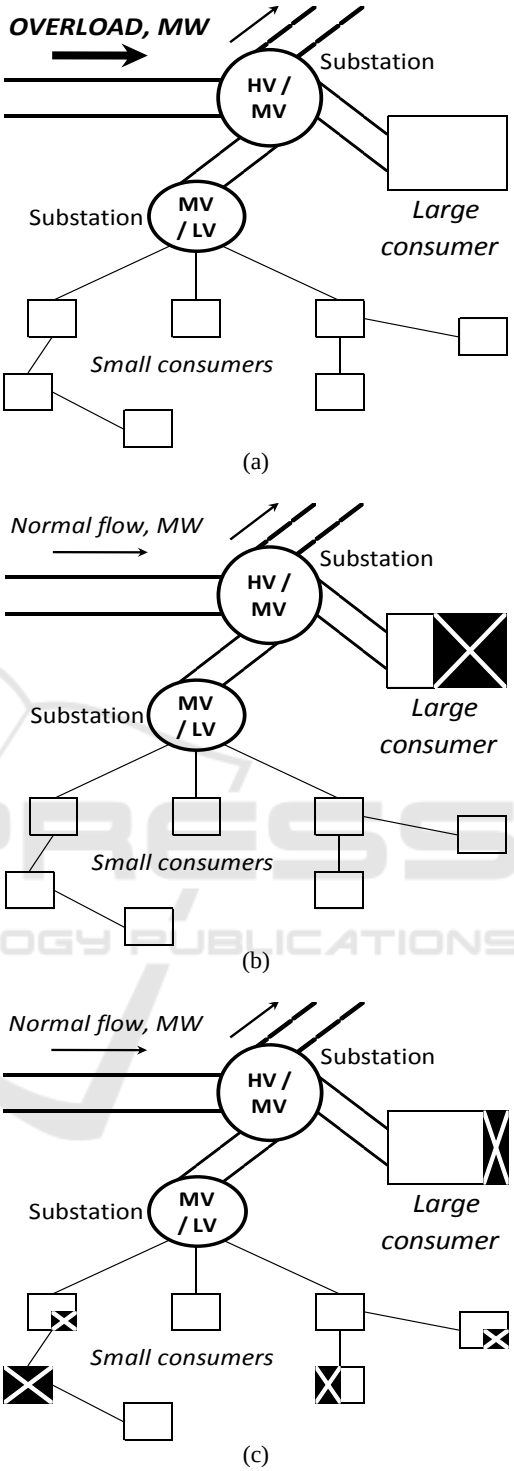

Figure 1: Possible control actions against overload of the line. Emergency situation – overload of the main line (a); Conventional control action – a large load partial shedding (b); Alternate control action – distributed load shedding (c).

Load shedding scheme is addressed, depending on appeared emergency situation, to provision of stability of the ties of main network or thermal stability, and stability of loads of controlled subsystem. Coming from the tasks to be fulfilled, the load shedding algorithms should be subdivided as follows (Voropai, 2018):

1. *Algorithms addressed to providing the stability of the ties of main network.* These algorithms are to operate with the close interaction with the centralized automatic stability control system. The automation operation under those conditions consists in the procedure of choice and consequent disconnection of required amount of the load. If the necessary amount of the load to be shed could not be collected from small consumers then load of large consumers be partially shed. To minimize the shedding, the more precise balancing is needed by means, among others, further splitting the steps of large consumers disconnection.
2. *Algorithms preventing the overload with the current of controlled subsystem lines.* These algorithms are to provide an optimal amount of load shedding, i.e. to minimize the cost of unloading the overloaded transmission line. The automation is to operate as an intellectual emergency control system providing the fast disconnection of the consumer's load in a minimal necessary amount to prevent the equipment overload.

Table 5: Summary of requirements to load shedding algorithms.

Requirements	Comments
1. Keeping the balance between complexity and simplicity of implemen-tation	– On the one hand, the algorithms are to be complex enough to provide an acceptable level of control action precision. – On the other hand, they are to be simple enough to provide an acceptable speed of calculations.
2. Providing a high level of fault tolerance	The algorithms do not fail in the case of uncritical loss of information. Should the loss of information be critical, the algorithms either implement the excessive control actions, or delegate control to power system operator.
3. High speed diagnostic self-testing	The possibility of implementing an effective self-testing procedure is related directly to the requirement of maximal simplification of the algorithms.

Coming from above analysis the requirements to load shedding algorithms can be summarized as in Table 5 (Voropai, 2018).

4 INFORMATIONAL SUPPORT OF INTELLIGENT CONTROL PROBLEMS

In the EnergyNet strategy, great significance is attached to the subsystem responsible for solving the problems dealing with control of the current operating conditions of intelligent power system. This subsystem includes the technical means for the acquisition, transfer and processing of data on the state of the network components and state variables (SCADA and WAMS), as well as the software for the calculation of current operating conditions (state estimation) of the EPS, forecasting and monitoring of operating parameters on the basis of the obtained information.

Simultaneously with the development of information technologies and orientation to the total digitalization of information exchange, the threats of cyber-intrusion into the management systems of the EPS are increasing. Cyberattack is deliberate physical damage of measuring sensors and transmission channels, malicious intrusion into local networks of the power enterprise for the purpose of entering of obviously false information, partial or complete blocking of a traffic, distortion in work of system of synchronization of time and so on.

The systems of data collection and processing – SCADA and WAMS– belong to the subsystems of the Smart Grid, which are most vulnerable to the physical failures and information attacks dangerous in terms of their consequences (Rihan, 2013; Ten, 2007). The PMU measurements, as well as SCADA measurements, need to be validated (Glazunova, 2011). Especially the requirement for their validation is important when cyber-attacks (CAs) occur at the power industry facilities. Along with the development of technical measures to detect cyber interference in the control system of the power facility, we offer the development of the state estimation algorithms.

State estimation is a statistical method of data processing which is used to filter the measurement errors and to calculate unmeasured variables. Detection of bad data and suppression of their influence on the state variable estimates are one of the most pressing issues when solving the state estimation problem. The results of state estimation, i.e. the steady state variables, represent the basis for

solving the problems of operating control of intelligent power system (EMS-application), including the problem of security calculation and analysis. The use of PMU measurements to solve the control problems requires measurement validation, which can be carried out on the basis of the state estimation methods. The method of test equations was developed to detect bad data in SCADA measurements, then adapted to check PMU measurements and analyze cyber security of SCADA and WAMS (Gamm, 2002; Kolosok, 2014). Test equations are steady-state equations which contain only measured variables y. When the values of measurements are written in such equation a discrepancy appeared due to the presence of random noise in those measurements. The TE method based on comparing the value of the discrepancy magnitude with some statistical threshold allows one to judge on the presence of gross errors in measurements. The TE method does exclude gross errors and replace erroneous measurements with pseudo measurements. The constant presence of gross error in a Test Equation during a long time period forces the operator to analyze the reasons for the corruption of initial data with subsequent generation of recommendations to compensate for the systematic errors in measurements or fix the fact of cyber-attack.

The TE technique is applied not only to bad data detection but to the SE problem too. To this end a set of measurements is divided into basic measurements and redundant ones. (The basic measurements are a minimum set of measurements that provide observability of electric power system.) First the estimates of basic measurements are calculated, after that – the estimates of redundant measurements and unmeasured variables are found out. The main advantages of the TE method are the opportunity to reduce the dimensionality of the problem and to use the obtained test equations for a priori detection of bad data in measurements. Unforunatelly, if cyber-attacks are nontrivial or a great amount of software and technical means appear to be attacked simultaneously, the state estimation method becomes ineffective.

In Energy Systems Institute SB RAS (ESI SB RAS) (Glazunova, 2011), we 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. Along with the traditional algorithm of the linear SE solved through the state vector, the proprietary algorithm of the linear SE by the TE method is developed in ESI SB RAS (Kolosok, 2014). Increase the redundancy of measurements and their accuracy greatly affects the results of data verification accuracy of estimates.

According to the above considerations we suggest the following technique to identify cyberattacks on SCADA and WAMS:

1. Local areas which are totally observable by PMU measurements are singled out in the scheme of an electric power system;
2. For such local areas the local state estimation is performed using linear algorithms with unconditional a priori verification of the initial data;
3. A great number of bad data in measurements or the measurements that go beyond the technological limits, measurements diagnosed as doubtful and unchecked (belonging to one facility), should mean a complete failure of PDC operation and initiate finding the reasons for such a failure;
4. If there are formal signs of a WAMS failure, an independent simultaneous (by one timestamp) bad data detection and state estimation by SCADA measurements are performed at this energy facility;
5. A sharp discrepancy between the results of the independent procedures for the WAMS and SCADA measurement verification are used to make a conclusion if there is a malicious attack on one or another system.

The efficiency of the suggested approach was tested using a fragment of the scheme equipped with SCADA and PMU measurements (Kolosok, 2018). The calculation network was divided into areas that have either a SCADA-server or a WAMS phasor data concentrator (PDC) at the center of each of them (Fig.2). The node 5 where both SCADA-server and PDC were installed becomes to be boundary one.

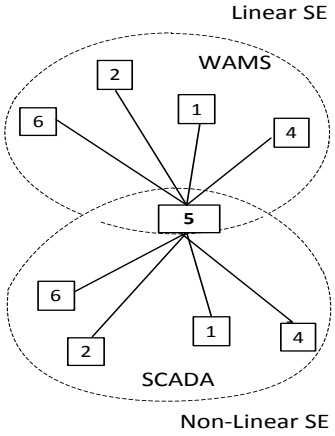

Figure 2: Dividing the area of node 5 on SCADA and WAMS.

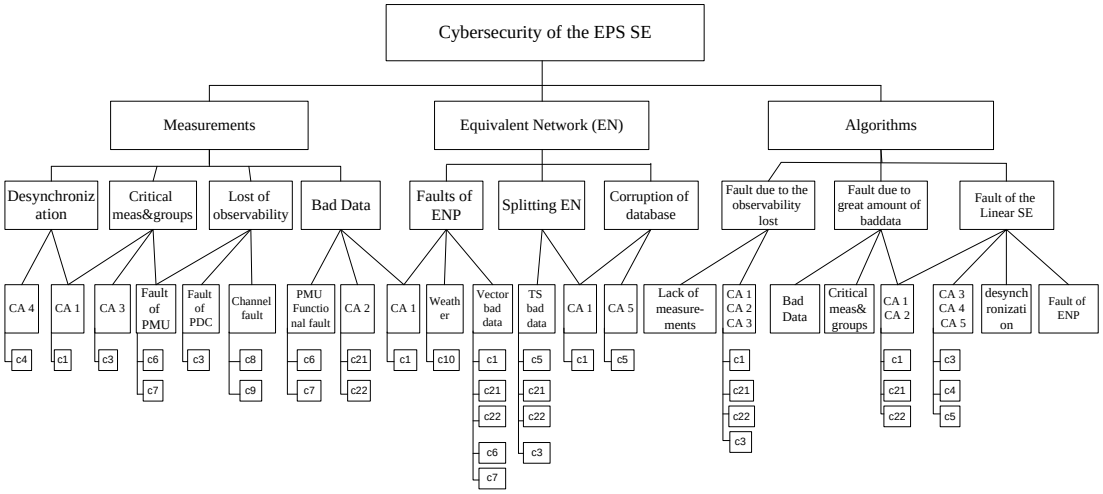

Figure 3: A tree of the power system state estimation software faults.

The results of bad data detection using two independent systems (SCADA and WAMS) and combination of a-priori and a-posteriori bad data detection make it possible to conclude whether or not there is a malicious cyberattack The efficiency of the suggested approach was tested using a fragment of the scheme equipped with SCADA and PMU measurements (Kolosok, 2018). The calculation network is divided into areas that have either a SCADA server or a WAMS concentrator at the center of each of them (Fig.2). The node 5 where PDC is installed becomes to be boundary one.

A problem of resistance of the state estimation procedure to cyberattacks on the system for gathering and processing of PMU measurements was investigated, and the SE procedure itself using an analytical approach to the assessment of SE software operability based on the fault tree technology. The Fault Tree of the SE cyber security consists of three main components: Measurements, Equivalent Network and Algorithms. The failure of any of these components may lead to a failure of SE procedure itself. Every component has elements, for example, {desynchronization of measurements; critical measurement and critical groups; loss of observability; bad data} in the first component, which are vulnerable to different potential cyberattacks (CA_i). The fault tree technology helps one make visual solution for constructing countermeasures c_{CA_i}.

At present the SE procedure is getting increasingly more important in the conditions of adjustment of the automated systems for acquisition of phasor measurements as well as in the conditions of various cyber threats. The SE mathematical tools allow us to straighten out a tangle of true and erroneous measurements and make certain conclusions on the operability of the devices for collection and primary processing of measurements.

An algorithm for a two-level SE on the basis of SCADA and WAMS measurements is effective in terms of detection of malicious attacks on energy system.

5 VOLTAGE/VAR CONTROL AND OPTIMIZATION USING AI APPROACH

In the nearest future the development of the networks in megalopolises and large industrial centers in Russia will result in the formation of systems with a complex multi-loop structure. In these conditions we should expect large-scale system emergencies which will occur according to the scenario in which the electrical current and voltage constraints become decisive in case of emergency operating conditions unfolding. The first system blackout of such kind happened in the UPS of Russia in Moscow power system in May 2005.

5.1 Multi-agent Approach

Traditional voltage and VAr control (VVC) and optimization (VVO) techniques has a number of downsides: low robustness to erroneous inputs; computational complexity, erroneous identification of states, etc (Tomin, 2018). In addition, the use of classical optimization techniques, such as linear programming or decoupled Newton-based optimal

power flow and mixed integer programming, usually provides limited the useful results as show in (AlRashidi, 2010). A relatively new approach to design the problem is the application of AI techniques, such as machine learning, multi-agent systems, fuzzy logic control, etc.

The approaches implemented on the basis of MASs as a whole have a single methodology of decentralized or partial decentralized (hybrid) control of electric power system (Sidorov, 2018). The principle of distributed intelligence is implemented at permanent or periodic exchange of messages among the agents to implement specified protocols. Any of the elements of a power grid (generators, loads, lines etc) could be modified to be an agent to provide specified protocols - tap changers block, load shedding, increasing of reactive power production etc. The examples of the completed developments in this area can be exemplified by a multi-agent control system (MACS) of voltage and reactive power control developed by Center of systems studies and development at JSC "STC FGC UES" Russia (Arkhipov, 2014) and ESI SB RAS, Russia (Sidorov, 2018; Kurbatsky, 2016).

In ESI SB RAS, we developed In ESI SB RAS, we developed MACS, which is provided a decentralized automatic Volt/VAr control associated with determination of the time of critical overload and switching to the load shedding procedure, rather than ensuring the best efficiency of secondary control. The agents are integrated by means of a common information environment in which they can exchange messages. The knowledge of an agent about subsystem is formed as a basis of sensitivity coefficients (elements of Jacobi matrix of steady-state equations).

A decentralized MACS was applied to make the generator agents (GAs) of a power system interact effectively to prevent voltage collapse. The GA receives the following local information: stator and rotor currents, bus voltages, the local stop-off signals, and the numbers of tap changers of the generator transformers. If the value of the stator or rotor current exceeds the maximum permissible value (approaching the limit value), the GA tries to exclude the possibility of switching off the generator due to overload. The condition for generator overload is the increase in the current generation of reactive power, Q_g above the maximum value, Q_{max}:

If the excitation current of the GA goes beyond its normal range, the GA tries to decrease it to exclude the possibility of generator tripping. The overloaded GA determines the rate of reactive power increase according to sensitivity coefficients. It is important to note that we do not need to know the exact value of the coefficients for the current conditions. If any of the requested GA stops increasing Q_g it informs the overloaded GA. If all the requested GA stop increasing Q_g but the overload is not eliminated, the overloaded GA starts the load shedding procedure.

5.2 Machine Learning Approach

Significant support in the development of system operator adviser intelligent systems involved the approaches based on the machine learning algorithms, namely artificial neural networks (ANNs) (Methods, 2010; Diao, 2009), decision trees (Kurbatsky, 2016; Zhukov, 2018), which have high approximating abilities. This made it possible to effectively train such models to successfully solve a whole complex of real-time problems within the framework of applications of automated management systems. The majority of solutions in this direction are connected with the transformation of the classical optimization problem into the regression /classification task, which allows to significantly reduce the computing time while maintaining acceptable accuracy. The most successful developments were obtained in the application of various decision trees algorithms for VVC/VVO.

In ESI SB RAS, we developed an online VVC/VVO technique based on the model of online decision trees (Proximity Driven Streaming Random Forest (PDSRF) (Zhukov, 2018) and deep learning models (DeepCS). The combination of original properties of machine learning and capabilities of voltage stability L-index indicator as a target vector makes it possible to reformulate typical VVO problem as a machine learning problem. Thus, we presented the classic optimization problem as a multi-output regression problem, which aims to simultaneously predict multiple real valued output/target variables. As a result, the obtained values of injections ΔQ from PDSRF or DeepCS were used for online VAR compensation by using reactive power sources, which decreased L_{sum}.

In (Zhukov, 2018) was clearly showed that the power system will work in the optimal operating condition when the sum of local L-indices, L_{sum}, is minimal. This AI update enables us to apply the classical methodology in real time.

5.3 Case Study

The efficiency of the proposed intelligent system were tested on IEEE 6 (Fig. 4) and IEEE 118 - Bus test systems. The proposed decentralised MACS are implemented in MATLAB/PSAT. PDSRF models is implemented in C++. DeepCS is implemented in Python using TensorFlow library. A set of the obtained system states was used to offline calculate the values of global L-index, and on the basis of L_{sum}, the reactive power injections were found for each load node.

At each step of the load increase in the IEEE systems, we simulated the following three cases of VVC:

1. Case 1 – local devices: overexcitation limiter (OEL) in AVR, there are no VAR compensators,
2. Case 2 – all generators have MACS agents for preventing generator overload, there are no VAR compensators
3. Case 3 – MACS + DeepCS or PDRSF (there are VAR compensators).

Figure 4 shows the location of all AI-elements in the IEEE 6 system: generators with AVR that are agents and loads with 25 Mvar VAR compensators that are controlled by machine learning models (PDRSF or DeepCS).

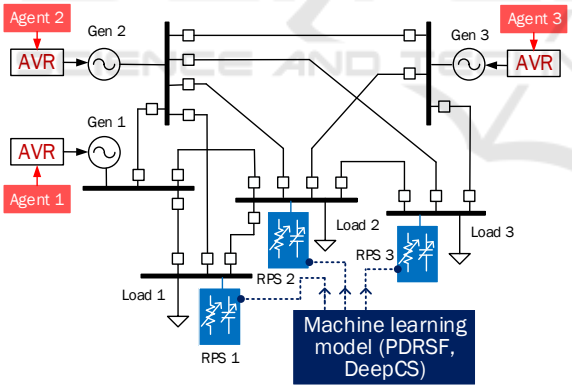

Figure 4: IEEE 6-Bus system with AI-grid elements.

Figure 5 demonstrates the simulation results. The use of MACS in Case 2 allows maintaining voltage stability at the critical step of overload and preventing voltage collapse. At load factor *N=19*, MACS starts the load shedding procedure, because all the requested agents stopped increasing Qg but the overload was not eliminated. The joint use of MACS and machine learning algorithms (PDRSG or DeepCS) in Case 3 allows us not only to optimize the voltage/VAR profiles before critical overload (secondary control stage), but also improve voltage profiles in emergency control stage of the IEEE 6-Bus system. Moreover, in this case, the load shedding procedure was started later (*N=22*) than in Case 2.

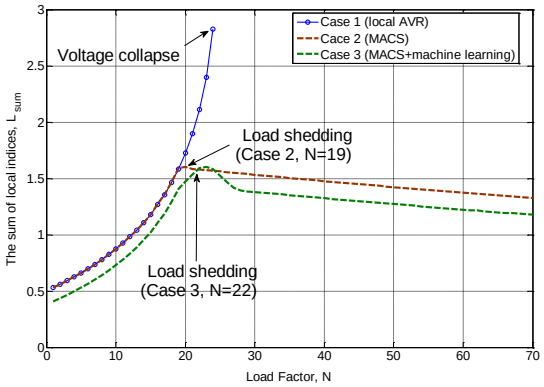

Figure 5: The curves L_{sum} for IEEE 6-Bus system.

As shown in Table 6, the DeepCS gives better results than PDRSF.

Table 6: Comparative test results for different multi-output regression models (IEEE-6 test scheme).

Models	**MAE x 10^{-3}, p.u.**		
	RPS1	RPS2	RPS3
PDRSF	0.385	0.456	1.126
DeepCS	0.087	0.034	0.540

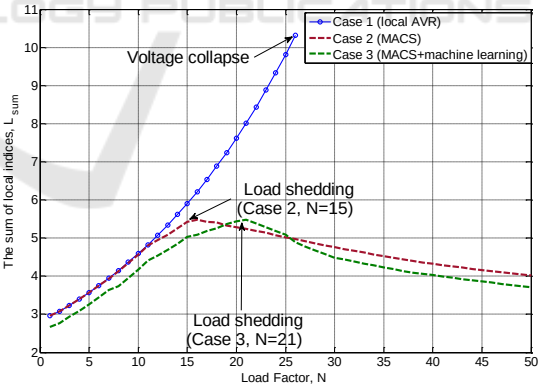

Figure 6: The curves L_{sum} for IEEE 118-Bus system.

The Case 1 modeling leads the IEEE 118 system to voltage collapse (Fig.6). Using MACS in the Case 2 allows to maintain voltage stability at the critical step of overloading and prevent the voltage collapse. Again, joint using MACS and machine learning algorithms in the Case 3 allow to optimize voltage/VAR profiles not only before critical overloading secondary and emergency control stages, as well as to postpone the start of load

shedding procedure for IEEE 118-Bus system. Thus, the use of the proposed hybrid AI technique (Case 3) provides intelligent secondary and emergency control making the large test system a more stability under disturbances.

The operability of the MACS in comparison with traditional local automatic was also tested using the IEEE 118-Bus (Fig. 7). The tests demonstrated a lower probability of cascading disconnection in the Case 2 where the MACS is used since the reactive power redistribution makes the loading of generators more balanced compared to the situation where there is no MACS at all (the Case 1). This happens because MACS is trying to redistribute the reactive power from overloaded to underloaded generators. To this regard, when using MACS the number of steps towards stability limit Nmax will always be bigger (N_{max}=255), compared with the situations without any automation (N_{max}=250) and with only local overloading control (N_{max}=221).

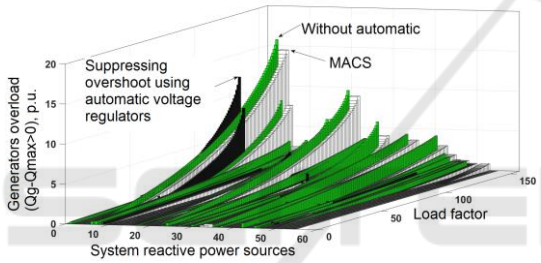

Figure 7: Results of quasi-dynamic modeling in the IEEE 118 test scheme. Comparison of equipment overload under different approaches.

6 CONCLUSION

Intelligent automation of electric power grid in large cities is a key contributor and a prerequisite to building the smart grids of the future. ESI SB RAS has been driving the development of advanced protection, supervision, control and management techniques and systems for the complete power delivery process.

The smart solutions are built on AI products for protection and control, monitoring, measurement, and communication. The creation of intelligent power system under EnergyNet platform should provide a qualitatively new level of efficiency of electric power industry development and functioning, raise system security, and increases the quality and reliability of the electricity supply to consumers in large cities.

ACKNOWLEDGEMENTS

This work was supported by the Russian Scientific Foundation (No.19-49-04108) and German Research Foundation (No. RE 2930/24-1) under the joint project "Development of Innovative Technologies and Tools for Flexibility Assessment and Enhancement of Future Power Systems".

REFERENCES

ABB Power and Automation: Solid Foundations for Smart Cities Available from: https://new.abb.com/docs/default-source/smart-grids-library/abb_smart_grids_white_paper_2013.pdf

Voropai, N., Kurbatsky, V., Tomin, N., Panasetsky, D., 2016. Improving power system monitoring and control in Russian modern megalopolises," 2016 18th Mediterranean Electrotechnical Conference (MELECON), Lemesos.

Efimov, D.N., 2011. Some developments, prospective ways and projects of smart grid technologies in Russia—an overview, Proc. of IEEE PES ISGT Europe 2011, Dec. 5–7, Manchester, UK

Voropai, N.I., Efimov, D.N., Etingov, P.V., Panasetsky, D.A. 2011. Smart emergency control in electic power system, 18th IFAC World Congress, Milano, Italy, Aug. 28–Sept. 2 (2011), Pp. 1658-1664

Voropai, N.I. et al., 2011. Emergency control in electric power systems based on smart grid concept, APPEEC'2011 Int. Conf., Wuhan, China, March 25–28.

Voropai N., Kurbatsky V. Tomin N. et al., 2018. Intelligent control and protection in the Russian electric power system / in: L. Lamont, A. Sayigh (eds) Application of Smart Grid Technologies. Case Studies in Saving Electricity in Different Parts of the World, Pp. 61-140

Efimov, D.N., 2012. Smart grid in Russia: today's and tomorrow's practices, Proc. of the 7th Conf. on Sustainable Development of Energy, Water and Environment Systems, Ohrid, Macedonia.

Budargin, O., 2010. Modernization via innovation development—creation of smart grid, Presentation for Commission on Modernization and Technological Development of Russian Economy, 2010 October, 26 (2010) (in Russian). Available from: http://www.fsk-ees.ru/media/File/press_centre/speeches/Presentation_Budargin_26.10.10.pdf

R&D Report, 2009. JSC "DALENERGOSETPROJECT" Main Directions for Development of Primorye Region Energy till 2012 and for Perspective to 2020 (2009), Vladivostok (in Russian)

Rihan, M., Ahmad, M., and Beg, M.S., 2013. Vulnerability Analysis of Wide Area Measurement System in the Smart Grid. Smart Grid and Renewable

Energy. Pp. 1-7. Available: http://www.scirp.org/ journal/sigre.

Ten, C., Liu C., Govindarasu, M., 2007. Vulnerability Assessment of Cybersecurity for SCADA Systems, in Proc. 24-28 June 2007 Power Engineering Society General Meeting.

Gamm, A., Kolosok, I., 2002. Test Equations and Their Use for State Estimation of Electrical Power System, Power and Electrical Engineering: in Scientific Proc. of Riga Tech. University. Riga: RTU, Pp. 99-105.

Kolosok, E. Korkina, E. Buchinsky, 2014. The Test Equation Method for Linear State Estimation Based on PMU Data, unpublished, presented at the 18th PSCC. Wroclaw, Poland.

Glazunova, A., Kolosok, I., Korkina E., 2011. Monitoring of EPS Operation by the State Estimation Methods, in "Innovative Smart Grid Technologies" (ISGT Europe-2011), Great Britain, Manchester, 5-7 December 2011.

Kolosok I.N., Korkina E.S., 2018. Decomposition of Power System State Estimation Problem as a Method to Tackle Cyberattacks / The1st IEEE International Conference on Industrial Cyber-Physical Systems (ICPS-2018), Saint Petersburg, Russia, May 15-18, 2018, SF-004928

Tomin N., Kurbatsky V., Zhukov A., Panasetsky D., Sidorov D., 2018. Voltage/VAR Control and Optimization: AI Approach, Proc. of 10th IFAC Symposium on Control of Power and Energy Systems, (CPES 2018), Meiji University, Tokyo.

AlRashidi, R., AlHajri, M.F., Al-Othman, A.K., El-Naggar, K.M., 2010. Particle Swarm Optimization and Its Applications in Power Systems, Pp. 295-324. Springer Berlin Heidelberg, Berlin, Heidelberg.

Voropai, N.I., Tomin, N.V., Sidorov, D.N. et al., 2018. A Suite of Intelligent Tools for Early Detection and Prevention of Blackouts in Power Interconnections // Autom Remote Control. Vol.79, Pp. 1741–1755

Arkhipov I.L., et al., 2014 Multiagent control system for voltage and reactive power, in Proc. Of the 22nd conference "Relay protection and automatics of power systems", Moscow. Pp. 243-252

A set of intelligent tools for prevention of large-scale emergencies in electric power systems / Voropai N.I., Kurvatsky V.G. et al. - Novosibirsk: Publishing House "Nauka", 2015 - 332 p. (in Russian)

Methods and models for power system reliability studies, Syktyvkar: Komi Scientific Center of Ural Branch of RAS, 2010, 292 p. (in Russian)

Diao R. at el., 2009Decision tree-based online voltage security assessment using PMU measurements, IEEE Trans. on Power Systems. Vol. 24, no. 2, Pp. 832-839.

Zhukov A. On-Line Power Systems Security Assessment Using Data Stream Random Forest Algorithm Modification / Zhukov A., Tomin N., Sidorov D., et al In: Zelinka I., Vasant P., Duy V., Dao T. (eds) Innovative Computing, Optimization and Its Applications. Studies in Computational Intelligence, vol 741. - 2018. Springer, Cham

Budargin, O., 2011. Smart Grid—First Outcomes, Presentation for Round Table "Smart Grid—Projects of Future", 2011 June, 16–18, 2011 (in Russian). Available from: http://www.fsk-ees.ru/upload/docs/ 01_ayladwlg.pdf

Fortov, V.E., and Makarov, A.A., 2012. *A concept of Russia's intelligent power system with active-adaptive network.* Moscow JSC "NTC FSC EES», 2012, 235 p. (in Russian)

National Standard P 55105-2012, 2012. United power system and isolated working systems. Operative-dispatch management. Automatic emergency control of modes of power systems. Emergency control of power systems. Norms and requirements. (in Russian)

National Standard P 55438-2013, 2013. United power system and isolated power systems. Operative-dispatch management. Relay protection and automation. Interaction of actors, consumers of electrical energy in creating (modernization) and the exploitation. General requirements. (in Russian)

Kolosok I., Korkina E., and Mahnitko A., "A fault tree cyber security analysis of power system state estimation software", in Proc. 2017 of the 9th International Scientific Symposium on Electrical Power Engineering, ELEKTROENERGETIKA, Pp. 349-353.