Development of Software for Modelling Decentralized Intelligent Systems for Security Monitoring and Control in Power Systems

Daniil Panasetsky, Nikita Tomin,
Nikolai Voropai, Victor Kurbatsky
Electric Power Systems Department
Melentiev Energy Systems Institute
Russian Academy of Sciences
Irkutsk, Russia
panasetsky@gmail.com, tomin.nv@gmail.com

Aleksei Zhukov, Denis Sidorov
Applied Mathematics Department
Melentiev Energy Systems Institute
Russian Academy of Sciences
Irkutsk, Russia
zhukovalex13@gmail.com, contact.dns@gmail.com

***Abstract*— With rapidly increasing complexity of power grids in Europe, North America and Asia, liberalization of electricity markets and increasing penetration of renewable energy, the risk of large-scale emergencies and blackouts increases. This paper proposes a novel approach for development of software for modelling of decentralized intelligent systems for security monitoring and control in power systems. The innovation here is to joint use the modern computing environments – MATLAB, R and Java Agent Development Framework platform. The proposed intelligent system was tested on the modified 53-bus IEEE power system**

***Index Terms*-- blackout, software design, power systems, emergency control, intelligent system, multi-agent system, machine learning**

I. Introduction

Recent history shows that no large-scale power system is exempt from a succession of complex and rare events that can lead to a collapse of a large part of the system or a major outage. In recent years, due to liberalization, power systems are being operated closer and closer to their limits. At the same time, they have increased in size and complexity. Both factors increase the risk of major power outages and blackouts [1]-[3]. Automatic emergency and operational control systems are required to prevent cascading emergencies and blackouts. Unfortunately, in many cases, the current generation of these systems is ineffective and unreliable. Recent examples of large-scale blackouts in North America in 2003, Moscow in 2005, Europe in 2003 and 2006, and India in 2012 testify to this.

A low level fault-tolerant of elements and lack of local devices coordination are the two main disadvantages of modern emergency control systems, which cause large-scale blackouts. Greater centralization of control systems and improving redundancy level (N-2, N-3) could help to handle these significant problems. However, excessive redundancy and centralization can lead to a cost increase and reliability decrease of emergency control systems due to improving structural complexity of systems elements.

A more promising solution is to use of decentralized adaptive control systems with simultaneous increase of the intelligent level of the local devices. Several studies used this approach against voltage collapse, current overload as well as for coordinated control of FACTS devices [4]-[7].

In emergency and abnormal conditions, a power system operator has to deal with a large amount of data and apply the most appropriate remedial actions. However, due to emotional and psychological stress, an operator may not be able to adequately respond to critical conditions and make correct decisions. Moreover, in emergency conditions, a vital decision must often be taken in a matter of minutes, sometimes even seconds. Mistakes can damage very expensive power system equipment or worse lead to the major emergencies and even catastrophic events. Clearly, there is a strong need for intelligent decision support systems for preventing major emergencies and blackouts in modern power systems. In competitive electricity market along with automation, computational intelligent techniques are very useful.

Traditional methods of security evaluation involve numerical solutions of nonlinear load of equations and transient stability analysis with detailed machine modelling for all credible contingencies. However, the complexity and size of modern power systems such that complete computational solutions usually cannot be obtained in a timely fashion, and thus cannot be used in emergency conditions for decision support [8], [9].

As a rule, the development of a new algorithm or approach to operational or emergency control includes the following set of steps:

- *Step 1.* Theoretical justification (conducting research, writing articles, etc.);

This work is funded by Russian Science Foundation (project No 14-19-00054)*)*

- *Step 2.* Development of the software required to validate the proposed algorithm (approach);
- *Step 3.* Implementation on prototypes (for example, the creation of hardware and software complexes);
- *Step 4.* Implementation of the algorithm (approach) in operation.

This paper proposes a novel approach for development of software (*Step 2*) in order to modelling of decentralized intelligent systems for security monitoring and control in power systems. The innovation here is to joint use the modern computing environments – MATLAB, R and Java Agent Development Framework (JADE) agent-based platform. The main goal of such combination is a creation (at minimal cost) of a single software complex for further checking of various decentralized adaptive algorithms of emergency control and monitoring systems (*Step 3*).

II. The specific requirements for intelligent emergency control systems

The authors have analyzed large-scale blackouts that occurred in 1965-2014 in the power interconnections of different countries. The analysis made it possible to identify the general regularities of their development, which are expressed in some typical phases: pre-emergency state, initiating events, cascading development of emergency, final state and restoration. It was established that the main types of emergency disturbances that occur in the quick phase of development were a voltage collapse and a considerable overload of equipment. The analysis showed that in the phase of initiating events the above-standard disturbances occur. The post-emergency conditions that occur at the end of this phase are off-design for the existing emergency control devices and for the dispatching personnel. Therefore, the existing emergency control systems furnished with the up-to-date automation means and the actions of System Operator may prove ineffective to prevent the subsequent catastrophic development of the emergency. The following drawbacks of the existing emergency control systems were noted [10]:

1. Lack of emergency control systems for reliable protection against voltage collapse;
2. Low resilience of the emergency control systems;
3. Lack of adaptability and coordination of local devices;
4. Critical redundancy of primary unprocessed data for the operator.

The conducted analysis revealed some flaws in the existing protection and emergency control systems that caused the catastrophic development of emergencies in the power interconnections [11]. The results of the studies testify to the necessity of the development of next-generation intelligent systems to complement modern emergency control systems, taking into account its "weak points" [9]. Based on the above said, the specific requirements for such intelligent emergency control systems have been developed. The systems should:

1. Have a tool for the intelligent monitoring and assessment of the power system operating conditions.
2. Be capable to predict potentially dangerous states of the power system.
3. Be highly resilient and able to coordinate local devices of emergency control system.
4. Have methods and models providing the protection of an electric power system with a complex structure.
5. Complement the existing ideology of emergency control systems but not contradict it.

In today's rapidly changing operating environment, conventional planning and operating methods can leave power systems exposed to failures. Developing solutions with computational intelligence tools offers two major advantages: development time is much shorter than when using more traditional approaches, and the systems are very robust, being relatively insensitive to noisy and/or missing data/information known as uncertainty. Intelligent management systems can play an advisory role suggesting the necessary actions, which should be taken to deal with a given emergency or abnormal condition as well as identifying failures of protection systems and circuit breakers.

III. Proposed Software Design

To meet the requirement of changing electric power grid security and stability analysis, a computational intelligence-based software development paradigm is proposed and deployed.

A. Programming paradigm

The choice of a programming paradigm is strongly influenced by the supporting programming language facilities and is an important task in software design. The development of software for power systems studies is usually focused on parallel and distributing programming. It is possible to classify a system as «parallel» or «distributed» using the following criteria [12]:

- In parallel computing, all processors may have access to a shared memory to exchange information between processors.
- In distributed computing, each processor has its own private memory (distributed memory). Information is exchanged by passing messages between the processors.

The final hardware implementation of an emergency control system that uses some distributed algorithms should be a set of independently operating devices with possibility of asynchronous transmission and reception of messages within an information environment – many computers at different substations connected through communication channels, this is a distributed computing. However, to simulate the behavior of this automation one must create a software system that consists of a set of special agents working in parallel; with the possibility of asynchronous messaging, this is a parallel computing.

In this way, the hardware implementation of a distributed emergency control algorithm is possible only based on distributed computing. However, a preliminary theoretical study of the algorithm can be effectively implemented only based on parallel computations.

Thus, a system modelling issue when used distributed control algorithms is to simulate the behavior of some number of devices (agents), each of which implements its own behavior. Agents must interact with each other, whereby the behavior of each should depend on the behavior of others. Effective implementation of this kind of computer model can be based on parallel computing using multi-agent and machine learning approaches.

Software implementation of such a system should include at least three main blocks: (1). a calculation module, which simulates the static and/or dynamic behavior of power system; (2) a program block, which simulates the complex behavior of agents: (3) a program block, which detect/forecast possible alarm states of power system.

There are two ways to develop the software necessary to implement a distributed emergency control algorithm:

- Creating from scratch software, which includes both calculation module and a module that provides parallel computing (simulating agent's behavior).
- Creating software that combines existing calculation module with existing agent platform.

From the viewpoint of efforts, the second method is much more practical. In this case, the problem of software development reduces to the problem of development of an interaction mechanism between agent platform and agent environment.

B. Software design comcept for modelling of an intelligent system

This paper proposes a parallel computing software design concept for modelling of an intelligent system, which combines the simulating and monitoring blocks with an agent-based platform (Fig. 1). The main purpose is to develop a mechanism of interaction between the simulating/monitoring tools and agent-based environment. Software implementation of the proposed intelligent system for preventing large-scale emergencies will consist of three parts:

- *power-system simulation tool* – a computer program that simulates the dynamic behavior of a power system (MATLAB © with open source Power System Analysis Toolbox (PSAT) tool);
- *security alarm tool* – a computer program for detecting/forecasting possible alarm states in a power system (programming/software environment R);
- *power security control tool* – a computer program that simulates the behavior of agents which provide distributed preventive/emergency control in a power system (JADE).

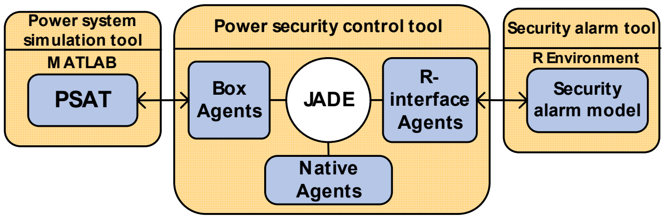

Figure 1. Simplified block diagram of the software realization for the proposed intelligent system.

C. Interaction mechanism

The power-system simulation tool is developed based on PSAT [13], which represents a software environment with an open code for operation on MATLAB platform or GNU/Otave. JADE is used as an agent platform for the research of power security control tool and interaction with security alarm tool (R environment) [14]. These environments and agent platform were chosen because they can be integrated using JAVA language. JAVA made it possible to completely transfer the modeling inside RAM memory, thus avoiding the necessity to use hard disc, which considerably accelerated the modeling process.

Furthermore, we decided to use the JAVA objects as an interaction mechanism. These objects are called box-agents (BA), which are the wrappers for data transferred from the MATLAB environment to each agent of the JADE system. Thus, the interaction between different software environments is organized by using interface agents that provide access to external software from multi-agent platform JADE through a network. The native agents are also formally identified as the agents which perform only inside platform (Fig. 1).

The main difficulty with the exchange of information between MATLAB, R and JADE environments is that BA are stored in a shared memory and without special measures all the applications have simultaneous asynchronous access to BA. This situation may cause a conflict, leading to a system crash.

In order to exclude non-synchronous access to BA, a special synchronization procedure was implemented. Selected mechanism is similar to one that is widely used for working with threads in JAVA. Its essence is to block one application to work with BA, while the second one is in the process of working with them, Figure 2.

After each step of integration MATLAB blocks all BA and goes into sleep mode until all BA will be unblocked by the JADE agents. Each agent in JADE environment registers the fact of his BA blocking. The agent processes the information contained in his BA, sends and receives all necessary messages and unblock the BA. When all BA are unblocked the calculation cycle is repeated again. The proposed mechanism provides synchronization and eliminates conflicts

R programming language is used as a computing environment for the security alarm tool modelling [15]. Communication with the R computing environment is carried out by using R-interface agent, which connects to specially created server based on Rserve. In the case of detecting an alarm state, R interface agent generates a request for execution of the corresponding code on R on the server in order to activate the power security control tool. Synchronizing mechanism for R-interface agent is similar to the described above.

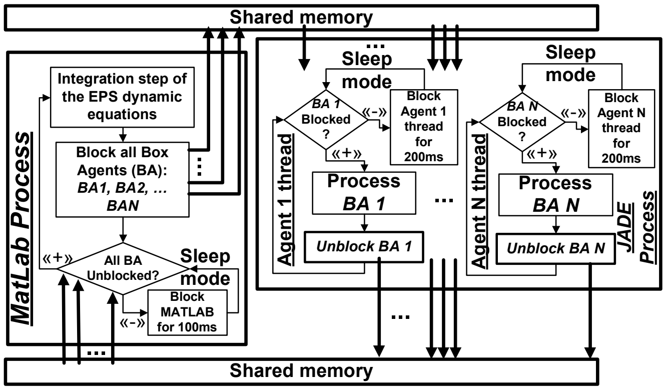

Figure 2. Simplified schematic diagram of BA synchronization mechanism

In result, the joint interface to connect power-system simulation, security alarm and security control tools was developed (Fig. 1). This is necessary for modelling of an integrated operation of the multi-agent control system with conventional power system controllers. This interface can use real-time measurements as inputs to the alarm and control tools; the output signal of the security alarm system can also activate the power security control tool.

IV. Intelligent System for Security Monitoring and Control

Based on the proposed software scheme, a novel intelligent system is developed (Fig. 3) [16], [17], which consists of two main parts: (1) the alarm trigger, an intelligent machine learning-based system for detecting possible alarm states in a power system, and (2) the multi-agent control system (MACS) for preventing large-scale emergency in a power system. The alarm trigger model is realized in R. The proposed multi-agent control system was implemented in JADE. MATLAB and PSAT are used as modeling tools.

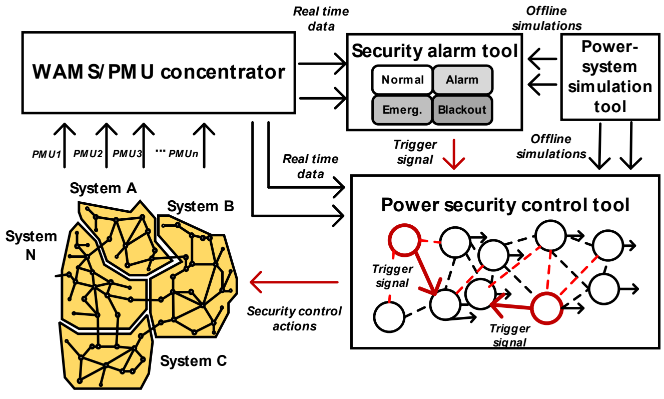

Figure 3. Block diagram of the proposed intelligent system.

A. *Security alarm system*

This paper is concerned with the real time identification of alarm states that are dangerous for the system security. The power system security monitoring concept is based on the classification of a power system state. We are examined a decision tree-based approach based on the random forest models [18], [19]. For more details on nonlinear dynamical systems identification and classification readers may refer to monograph [22]. A random forest-based alarm model is able to classify power system states in real time and, if required, to produce an alarm. The output signal of the security alarm system can activate the MACS with using of R-interface agent.

Under the off-line mode, security alarm model is trained using a set of training examples based on randomly generated events in a power system. Events are all generated by offline simulations using the PSAT. For each operating scenario considered, N-1 contingency case (line/generator/transformer outages) is simulated. The system information is periodically checked and updated in order to account for changing system states as accurately as possible so that the off-line trained alarm model may continue to perform well on the new system states. The final random forest-based model is used on-line to classify the system operating state based on the patterns created in the off-line and update modes.

B. *Multi-agent control system*

The concept of MACS is based on a decentralized structure that provides fast and robust responses in both normal and emergency conditions [6], [10]. The MACS provides reactive power control by coordinating the operation of different discrete and continuous control devices in a post-disturbances period in order to prevent voltage collapse in power systems. In this proposed system, it is assumed that all serial devices of the power system such as generators, transmission lines, transformers and power flow controllers are equipped with agents.

In this paper, for simplicity we assume that MACS includes two types of agents: generator agents (GA) and load agents (LA). The behavior of GA and LA is represented by finite-state machines. Certain events make the machines transition from one state to another. The GA uses information about the generator active and reactive power outputs, excitation current, primary/secondary voltages of the generator transformer, transformer tap position and alarm trigger from security alarm system. etc.

If, for example, the excitation current is close to its maximum limit, the GA decreases the current in order to prevent the generator tripping. Then GA communicates with other agents so that the problem of reactive power shortage in the system can be addressed. The LA receives information about power flows, primary and secondary voltages of the load transformer, transformer tap position, etc.

If agents receive an alarm trigger from security alarm system, the MACS can initiate the special collaborative protocol, in which the agents communicates and exchange information to evaluate possible exceeding the specified normal limits within their jurisdictions. They assess the severity of the situation, and if required produce appropriate remedial control actions to prevent blackouts.

Both types of agents have two objectives: local – maintaining local state variables within normal operational limits, and global – preventing large-scale emergency. Agents communicate with each other by using a communication language.

V. Simulations

A. Test power system

We demonstrated the approach on the modified IEEE One Area RTS-96 power system [20]. The modified test system (Fig. 4) had 53 buses and dynamic elements to represent generators and loads. Each load was modelled as an exponential recovery load [21]. Active power flow is directed from Subsystem B (230 kV network) to Subsystem A (138 kV network). Subsystem A is a low-voltage distribution subsystem being in near stressful conditions because of reactive power shortage, which potentially may cause voltage instability.

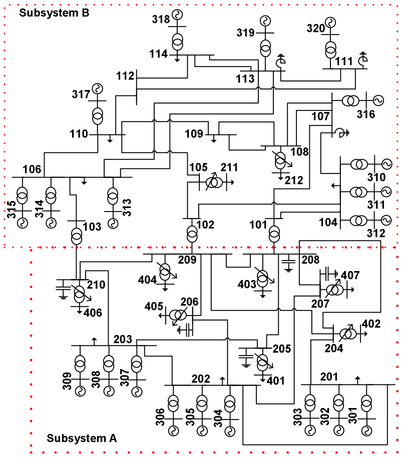

Figure 4. The modified IEEE One Area RTS-96 system.

The test system included the following features: (1) All transformers 230/138 kV were equipped with on-load tap changers (OLTCs). The OLTC time delay for the first tap movement was 20 s, and for subsequent tap movements is 5 s. The OLTP tap range is ± 12 steps. (2) Each generator was modelled by dynamic models of the 6th order, and equipped with Type I turbine governor (TG) and Type II automatic voltage regulator (AVR) (see [13]). (3) Machines connected to buses 301–309 were equipped with over-excitation limiters (OXLs) with a maximum voltage output signal of 0.1 (see [13]). (4) For simplicity, we assumed that the system does not employ under-voltage load shedding.

B. Case study

The proposed *decentralized intelligent control system* includes the security alarm system and MACS. In addition to the set of local controllers (TGs, AVRs and OXLs on each generator, and OLTCs on transformers connected to buses 204–210), it also includes OLTCs on transformers connected to busses 101, 102 and 103 (Fig 5). This test system was used to model different emergency scenarios.

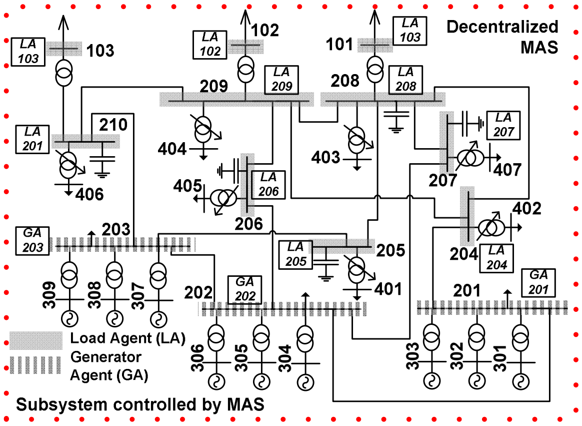

Figure 5. Subsystem A with installed Load Agents and Generator Agents

For example, the loss of generator G303 (t=5 s) leads to an uncritical increase of reactive power shortage in the subsystem B (Fig. 6). The alarm state is detected at this time. t=15 s – the tripping of transmission line Bus 103 – Bus 106 leads to overload of generators at bus 203. As soon as the security alarm model detected the serious alarm state (t=15.3 s), the MACS was activated to prevent the system from further deterioration. The MACS increased reactive power output until the excitation currents of the overexcited generators on bus 203 decrease to the near-critical values. In this case, the stability was maintained without load shedding. From t=170 s, the security alarm system identifies the normal state.

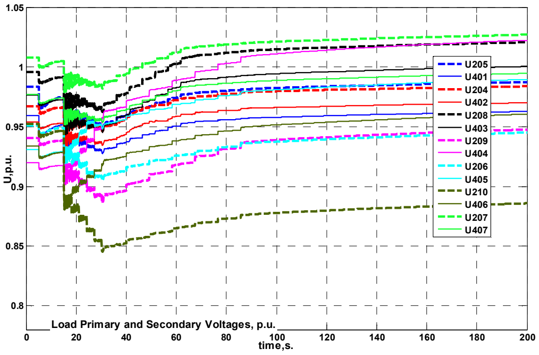

Figure 6. The system voltage profile (t=5 s – the loss of generator G303, t=15 s – the outage of transmission line Bus 103 – Bus 106)

Consider another scenario of the emergency disturbance. The outage of transmission line Bus 105 – Bus 110 (t=5 s) leads to the weakening of the power transit subsystem A – subsystem B (Fig. 7). The alarm state is detected at this time. Subsequent tripping of line Bus 107 – Bus 101 at time = 15 s leads to sharp decrease of active and reactive power transfer to subsystem B. The security model detected the serious alarm state (t=15.3 s) and produce alarm trigger. MACS rapidly identifies the absence of possibility to support voltage by reactive power sources coordination and triggers the load shedding procedure. However, the alarm state is also still activated because the system is still in the normalization of post-emergency state.

Thus, the use of the developed intelligent system based on the proposed software design in the modeled emergency scenarios makes it possible to maintain the stability of the test system through control actions owing to the coordination of reactive power sources and load scheduling.

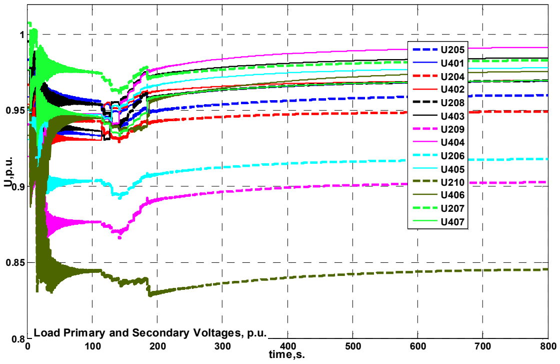

Figure 7. The system voltage profile (t=5 s – the outage of transmission line Bus 105 – Bus 110; t=15 s – the outage of transmission line Bus 101 – Bus 107.)

In terms of practical uses, an intelligent system will provide an additional automatic tool for power system security monitoring and control, which is targeting a blackout prevention scheme. The intelligent tool, on the one hand, will minimize the threat of large-scale emergencies, and, on the other hand, complement the existing emergency control ideology. The system will be also useful exploited by the power engineers in the context of off-line studies and as an analysis tool for on-line operation.

VI. Conclusions

This paper proposed a novel approach for development of software in order to modelling of decentralized intelligent systems for security monitoring and control in power systems. The basic idea is to joint use the modern computing environments – MATLAB, R and JADE. Software implementation of the proposed intelligent system consists of three parts: (1) power-system simulation tool, (2) security alarm tool, (3) power security control tool. The proposed software design scheme is tested on the IEEE One Area RTS-96 power system.

The innovation of the proposed software design is to develop new algorithms and implementation principles of an intelligent emergency control based on machine learning-based models and decentralized adaptive models that can effectively prevent voltage instability before they lead to major blackouts and overall collapse of the system. The proposed scheme of pre-emergency control will be able to preserve the integrity of a large-scale power system in an automatic mode and maintain a high level of a power system security. Development and implementation of the software prototype will make a significant contribution into a critical technologies development by: (1) development of new generation of "smart" emergency algorithms within the creation of Smart Grid concept; (2) advancement of technologies for preventing and eliminating man-made disasters in power systems.

References

[1] IEEE PES PSDP Task Force on Blackout experience, mitigation, and role of new technologies, blackout experiences and lessons, Best practices for system dynamic performance, and the role of new technologies, IEEE Special Publication 07TP190, July 2007.

[2] M. Negnevitsky, N. Voropai, V. Kurbatsky, N. Tomin, D. Panasetsky, “Development of an Intelligent System for Preventing Large-Scale Emergencies in Power Systems”, IEEE/PES General Meeting, Vancouver, BC, Canada, 21-25 July 2013.

[3] G. Trudel, J.-P. Gingras, J.-R. Pierre, “Designing a reliable power system: The Hydro-Qubecs integrated approach,” in Proc. IEEE, vol. 93, no. 5, pp. 907917, May 2005.

[4] M. Negnevitsky, N. Tomin, D. Panasetsky, V. Kurbatsky, “Intelligent Approach for Preventing Large-Scale Emergencies in Electric Power Systems”, IEEE International Conference on Electric Power Engineering PowerTech 2013, Grenoble, France, 16-20 June 2013.

[5] U. Häger, C. Rehtanz, N. Voropai: “ICOEUR Project Results on Improving Observability and Flexibility of Large Scale Transmission Systems,” IEEE PES General Meeting, July 2012, San Diego, USA.

[6] D. Panasetsky, N. Voropai “A Multi-agent approach to coordination of different emergency control devices against voltage collapse”, IEEE International Conference on Electric Power Engineering PowerTech 2013, Buharest, Romania, June 28-July 2, 2009.

[7] D. Panasetsky, N. Tomin, Y. Dechang; V. Kurbatsky, "A new intelligent algorithm for load shedding against overload in active distribution networks," Power System Technology (POWERCON), 2014 International Conference on , vol., no., pp.1677,1684, 20-22 Oct. 2014.

[8] L. Wehenkel “Machine-Learning Approaches to Power-System Security Assessment”, Dissertation, University of Liège, 1995.

[9] M. Negnevitsky, N. Tomin, Ch. Rehtanz “Preventing Large-Scale Emergencies in Modern Power Systems: AI Approach”, Journal of Advanced Computational Intelligence and Intelligent Informatics, Vol. 18, No.5, 2014.

[10] D. Panasetsky “Improving the structure and algorithms of emergency control in power systems to prevent voltage collapse and cascading line outages”, Dissertation, Melentiev Energy Systems Institute, 2014.

[11] Voropai N., Negnevitsky M., Tomin N., Panasetsky D., Rehtanz Ch., Haeger U., Kurbatsky V., "Intelligent Systems for Preventing Large-Scale Emergencies in Power Systems" Theoretical and Scientific Journal “Electrichestvo”, Vol.8, 2014 (In Russian).

[12] D. Peleg “Distributed Computing: A Locality-Sensitive Approach”, Society for Industrial and Applied Mathematics, Philadelphia, PA, USA, 2000, 343 p.

[13] Power System Analysis Toolbox. Documentation for PSAT version 2.0.0, February 14, 2008.

[14] F. L. Bellifemine, G. Caire, D. Greenwood “Developing Multi-Agent Systems with JADE”, John Wiley & Sons Ltd, 2007, 300 p.

[15] R: A Language and Environment for Statistical Computing, The R Core Team, version 3.1.3 (2015-03-09).

[16] M. Negnevitsky, N. Tomin, D. Panasetsky, and V. Kurbatsky, “Intelligent Approach for Preventing Large-Scale Emergencies in Electric Power Systems”, IEEE International Conference on Electric Power Engineering PowerTech 2013, Grenoble, France, 2013.

[17] M. Negnevitsky, N. Tomin, D. Panasetsky, U. Haeger, N. Voropai, Ch. Rehtanz, V. Kurbatsky "Preventing Large-Scale Blackouts in Power Systems Under Uncertainty", in Proc. of 18th PSCC, Wroclaw, August, 2014.

[18] L. Breiman “Random Forests”, Machine Learning , 2001, 45(1), pp .5-32

[19] N. Tomin, A.Zhukov, D.Sidorov, V. Kurbatsky, D. Panasetsky, V. Spiryaev “Random Forest Based Model for Preventing Large-Scale Emergencies in Power Systems”, International Journal of Artificial Intelligence, Vol. 13, No. 1, 2015, pp. 211-228

[20] J. M. S. Pinheiro. C. R. R. Dornellas. M. Th. Schilling. A. C. G. Melo “Probing the new IEEE Reliability Test System (Rts-96): HI-II Assessment,” IEEE Trans. Power Systems, Vol. 13, No. 1, 1998, 171.

[21] D. Karlsson, D.J. Hill. "Modelling and identification of nonlinear dynamic loads in power systems," Power Systems, IEEE Transactions on , vol.9, no.1, pp.157, 166, Feb 1994.

[22] D.Sidorov “Integral Dynamical Models: Singularities, Signals and Control”. World Scientific Series on Nonlinear Science. Series A, Vol.87. 2015, 243 p.