UDK 685.1

E.V. BREZHNEV[1], V.S. KHARCHENKO[2]

[1]*Centre for Safety Infrastructure Oriented Research and Analysis*
[2]*National Aerospace University KhAI, Kharkiv, Ukraine*

GRID SAFETY ANALYSIS BASED ON LINGUISTIC BAYESIAN BELIEF NETWORK

The state of power grid is determined by states of its systems, conditioned by their mutual influence of different nature. These influences cause the change of state of each system during grid life cycle. The proposed approach is based on application of Bayesian Belief Network, where nodes represent different grid systems, and links are stipulated by different types of influences (physical, informational, geographic, etc). The grid safety is evaluated on its criticality. The criticality and influence are treated as the linguistic values. It is suggested to evaluate criticality of system, considering the change of criticalities of all connected systems. Conditional probabilities are also represented by linguistic values. To demonstrate the approach to the grid safety analysis, Russian Sayano–Shushenskaya hydro power station accident is reviewed.

***Keywords**: Power grid, Computing with words, Safety, influence, Bayesian Belief Network*

1. Introduction

1.1. Motivation

The power grid (PG) is an interconnected network composed of power-generation stations, high-voltage transmission lines, lower voltage distribution systems, and other support components. PG is a highly controlled, dynamic and distributed network combined of different systems. This complexity of engineered systems is a consequence of several factors: the sheer size and interconnectivity of the PG, the safety requirements, the need to balance electricity supply and consumption throughout the grid at all times, and the nature of electricity – that it is generated as it is used. This means the PG requires continual surveillance and adjustment to ensure supply always matches demand.

Disturbances in PG operation can originate from natural disasters, failures, human factors, terrorism, and so on. Outages and faults will cause serious problems and failures in the interconnected power systems.

Therefore, it is of high priority to consider PG safety, mutual influence of its systems and forecast possible accidents and failures, considering their severity and high costs of recovery.

1.2. Work Related Analysis

There are a lot of approaches and techniques of PG safety assessment. An approach to PG safety analysis, taking into consideration technical, organizational, and individual aspects, is proposed in [1]. The PG safety analysis is supplemented by a set of geographic and economic aspects in [2]. An approach for PG safety assessment, based on processing statistical data related to PG operation, is proposed in [3]. The main task of the safety statistical analysis is to determine the failure probability distribution function and to assess power grid risk. Lack of statistics prevents the use of traditional statistical methods for PG safety assessment.

Beside well known techniques of probabilistic and deterministic PG safety analysis, there are a lot of different approaches used for PG safety assessment. Logic methods (Fault Tree Analysis and Event Tree Analysis), used for safety analysis, are applied in [4, 5]. Typical PG safety analysis techniques are connected with equipment failure analysis, environment and human factor. Nowadays, a new type of grid hazards – intentional attacks occur. This type of hazards is analyzed by the use of probabilistic approach together with conditional probabilities calculation. However, mutual influence of systems, taking into account dynamical aspects of functioning and variation of risks caused by their failures, is not considered. Recently, network modeling has been revived due to computer technology progress and increase of interest in complex systems analysis. Achievements in a graph theory for complex systems analysis are reviewed in [6]. A topology of North American Power System is analyzed. Graph is used as a model in [7]. Evaluations, specifying Power System topology, lack of connectivity, while demounting vertexes that connect transmitting substations, are calculated. Two types of power grid safety hazards are analyzed: random failures and antagonistic (intentional) attacks.

Some methods used for PG safety analysis are qualitative and based on expert evaluations. Analysis results are represented in the form of risk matrix, containing failure effect frequency and severity. Qualitative techniques of safety analysis do not operate numeric data providing results as descriptions, recommendations. The safety assessment is related to qualitative

description of frequency of undesired events, damage and threat scenario. In [8] it is specified that safety of a PG can be improved by implementing of process automation in disturbance situations.

The PG safety is affected by many factors regarding its design, manufacturing, installation, commissioning, operation and maintenance. Consequently, it may be extremely difficult to construct a complete mathematical model for the system in order to assess the safety because of inadequate knowledge about the basic failure events. This leads inevitably to problems of uncertainty in PG safety assessment.

As an application of probability theory, Bayesian belief network (BBN) [9] is a powerful tool both for graphically representing the relationships among a set of variables and for dealing with uncertainties in such variables. Many applications have proven that BBN is a powerful technique for reasoning relationships among a number of variables under uncertainty. BBN was successfully applied to ecological risk assessment and fault diagnosis in complex nuclear power systems.

But traditional BBN requires too much precise information in the form of prior and conditional probability tables, and such information is often difficult or impossible to obtain. In particular, in dealing with indirect relationships, even domain experts may find that it is usually difficult to make precise judgments with crisp numbers, that is, to assign an exact number to the probability that consequences happen given the occurrence of an event. In certain circumstances, a verbal expression (e.g. "very unlikely") or interval value (e.g. (0.15, 0.20)) of probabilistic uncertainty may be more appropriate than numerical values. Common disadvantages of mentioned approaches are as follows: PG safety is considered a static attribute; no consideration provided for mutual influences between power grid systems; there is a lack of publications for PG safety assessment with BBN using linguistic experts' judgments.

1.3. Goal of the Paper

To assure PG safety, it is necessary to consider and thoroughly analyze the nature of interaction among PG systems. The goal of the paper is to introduce an approach to power grid safety assessment, considering the different type of influence among its systems and evaluate safety using linguistic BBN. This technique can be useful to evaluate PG safety, taking into consideration mutual influences of its systems when all data available are represented by expert's knowledge.

2. Principles of grid safety analysis with linguistic bayesian network

2.1. General Principles of Analysis

The PG safety analysis is carried out taking into consideration principles of dynamism, hierarchy, uncertainty, and influence (interaction) of subsystems.

Principle of dynamical analysis assumes to record changes of system criticality during the operation as a result of changes of its states (transition to state of non-operability). At each stage of life cycle the criticality assessment specification and adjustment of criticality matrices [10], taking into consideration probable changes, are carried out.

The principle of hierarchy assumes representation of grid structure as a hierarchy. The set of criticality matrices of subsystem failures groups in clusters.

The principle of influence of subsystem failures of i-level (on subsystem failure criticality of the same level) and influence on subsystems of (i-1)-level (higher) is important.

The safety of all influenced subsystems must be reconsidered.

The principle of uncertainty takes into consideration information incompleteness and uncertainty related to the conditions that cause PG accidents.

The PG safety is an integral value composed of grid systems safety values. The grid safety is determined by uncontrolled mutual influence among grid systems. It is worth to note that influence exists on all grid levels and have to be taken into consideration when providing grid systems safety.

2.2. Types of Influences between power grid systems

According to the principle of influence, all influences (or relationships), existing in PG, can be divided into several hierarchy levels. The influence is an ability of one PG system to determine the state, characteristics or processes in other systems. Any type of influence is a time dependent value. The changes in NPP state and characteristics stipulate the changes in the influence value.

Generally, influences could be classified into different types [11]:

– Physical $I_{phys}(S_1 \to S_2)$ – a physical reliance on electricity flow between PG systems S_1 and S_2;

– Informational $I_{inf\,orm}(S_1 \to S_2)$ – a reliance on information transfer between power grid systems S_1 and S_2 (via through I&C systems);

– Geographic $I_{geograp}(S_1 \to S_2)$ – a local event occurred in PG system S_1 affects power grid's system S_2 due to physical proximity;

– Logical $I_{log\,ical}(S_1 \to S_2)$ – an influence that exists between power grid systems S_1 and S_2 that does not fall into one of the about categories;

– Organizational $I_{organiz}(S_1 \to S_2)$ (influences through policy, regulation, markets). An influence that exists due to policy or procedure that relates a state

change in one elements of PG to subsequent effect on other systems;

– The societal influence $I_{soc}(S_1 \to S_2)$ that one PG system may have one of societal factors as public opinion, fear and confidence, for example, staff of other PG system.

The formalization of influences between PG systems is very helpful for its safety assessment based on criticality matrices. Generally, criticality matrix is represented as FMECA table. The traditional FMECA [12] is the most widely used reliability analysis technique on the initial stages of system development.

For example, if PG system S_1 consists of three subsystems S_{11}, S_{12}, S_{13} then criticality matrix which represents the system S_1 might be presented as shown in the table 1.

Table 1

Criticality matrix for system S_1

System S_1		Severity of failure mode		
Failure rate		H	M	L
	H		S_{12}	
	M			S_{13}
	L	S_{11}		

Traditionally, the criticality assessment is performed by calculating the criticality accident (failure) as a product of its severity and probability:

$$Crt(S_i) = P(S_i) \times Sev(S_i), \quad (1)$$

where Si is PG system; P(Si) is probability of Si accident; Sev(Si) – severity of accident consequences.

According to the principle of hierarchy, the grid structure might be represented as a hierarchy. In this case, the safety of PG systems of higher level hierarchy might be evaluated as a sum of criticalities of power grid systems of lower level hierarchy. For example, considering the criticalities of S_{11}, S_{12}, S_{13} as subsystems of S_1, its criticality could be calculated as:

$$Crt(S_i) = P(S_1) \times Sev(S_1) + P(S_2) \times Sev(S_2) +$$
$$+P(S_3) \times Sev(S_3) = \sum_{i}^{I} P(S_i) \times Sev(S_i). \quad (2)$$

It is suggested to treat criticality as PG system's safety inverse value. The more system's criticality the less its safety.

It should be noted that criticality matrix might be used to represent different states of environment and its influence on PG systems. Any natural disaster might be evaluated in terms of their probability and severity for the nearest PG systems. These probabilities of system accidents (natural disasters) and its severity could be handled as linguistic or numerical variable. Hence, criticality is also treated correspondently either linguistic or numerical variable.

A linguistic variable is characterized by a quintuple (x, T(x), U, G, M) in which x is the name of variable; T(x) is the term set of x, that is, the set of names of linguistic values of x with each value being a fuzzy number defined on U; G is a syntactic rule for generating the names of values of x; and M is a semantic rule for associating with each value its meaning.

The set of state Ω_{S_i} of any PG system S_i is determined as:

$$\Omega_{Si} = \{Crt(S_i)=High, Crt(S_i)=Medium, Crt(S_i)=Low\}. \quad (3)$$

Any accident or failure of power grid system leads to the change of criticality of all connected systems. When a failure of one system occurs, the criticalities of all dependent systems are recalculated.

The prognosis and assessment of PG system service life, based on real time measurements, will help to identify grid systems most likely to fail. The potential estimation methods and equipment service life prediction for complicated systems consist of deterministic, statistical, physical-statistical and methods based on expert knowledge. These methods are used to predict the probability of accident of any system S_{ij} of S_i.

This criticality assessment is used to support the subjective expert judgment expressed by linguistic variable on the initial power grid system state. The more system criticality calculated on (2) the more confident expert's opinion on the criticality of each node of PG.

2.3. Bayesian Belief Network as a model for power grid's safety assessment

A classical BBN is a pair N= {(V, E), P} where V and E are the nodes and the edges of a Directed Acyclic Graph (DAG), respectively, and P is a probability distribution over V.

Discrete random variables

$$V = \{X_1, X_2, ..., X_n\}$$

are assigned to the nodes while the edges E represent the causal probabilistic relationship among the nodes. Each node in the network is annotated with a Conditional Probability Table (CPT) that represents the conditional probability of the variable given the values of its parents in the graph. The CPT contains, for each possible value of the variable associated to a node, all the conditional probabilities with respect to all the combinations of values of the variables associated with the parent nodes. For nodes that have no parents, the corresponding table will simply contain the prior probabilities for that variable.

The principles behind BBN are Bayesian statistics and concentrate on how probabilities are affected by both prior and posterior knowledge. In order to extend the classic BBN into fuzzy BBN which is capable of

dealing with linguistic variables, fuzzy numbers and their operations must be used.

The state of each PG system is determined by types of influence mentioned above. The figure 1 represents a fragment of network, which characterizes the PG, where S_1, S_2 are the parent nodes and system S_3 is a child node.

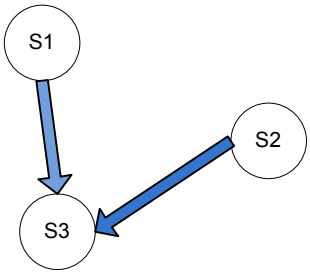

Fig. 1. A fragment of network, which characterizes PG

Generally, the several BBNs might be required to represent only one PG. These networks have the same nodes as PG systems, but different types of influence, which stipulate the different causal links (physical, geographical, organizational, logical, informational and societal) between nodes.

The different types of influence are characterized by its own weight. The more weight of the given type of influence the more PG is sensitive to this type of influence's loss. Apparently, the physical influence is more important, when PG safety is considered. But all types of influences should be considered to provide more accurate PG safety evaluation. For each type of influence might be introduced its own type of PG system particular criticality. It means that PG could be more vulnerable to the change of one type of influence and, at the same time, be insensitive to other type influence change.

Considering the types of influence mentioned it is assumed that the total PG system criticality is a function of power grid system's particular criticalities, stipulated by the particular types of influence, i.e.

$$\mathrm{Crt}^{\mathrm{total}}(S_i) = f(\mathrm{Crt}^{\mathrm{org}}(S_i),\ \mathrm{Crt}^{\mathrm{phys}}(S_i),\ \mathrm{Crt}^{\mathrm{georg}}(S_i),\ \mathrm{Crt}^{\mathrm{log}}(S_i),\ \mathrm{Crt}^{\mathrm{soc}}(S_i),\ \mathrm{Crt}^{\mathrm{inf\,orm}}(S_i)), \quad (4)$$

where $\mathrm{Crt}^{\mathrm{total}}(S_i)$ – the total power grid system criticality; $\mathrm{Crt}^{\mathrm{org}}(S_i)$ – particular criticality of power grid system, conditioned by organizational influence in PG; $\mathrm{Crt}^{\mathrm{phys}}(S_i)$ – particular criticality of power grid system, conditioned by physical influence in PG; $\mathrm{Crt}^{\mathrm{log}}(S_i)$ – particular criticality of power grid system, conditioned by logical influence in PG; $\mathrm{Crt}^{\mathrm{inf\,orm}}(S_i)$ – particular criticality of power grid system, conditioned by informational influence in PG; $\mathrm{Crt}^{\mathrm{soc}}(S_i)$ – particular criticality of power grid system, conditioned by societal influence in PG.

Depending on the scale used to evaluate criticality, each PG system could be characterized by the tuple of its criticalities values, considering the types of influence, which determine these criticalities. Example of power grid system criticality tuple is shown in the table 2.

Table 2.

Example of power grid system criticality tuple

PG S_i	Type of influence					
	Physical	Informational	Geographic	Logical	Organizational	Societal
	Criticalities caused by the given type of influence					
PG S_1	H	H	M	L	L	L
PG S_2	H	M	M	L	L	H
…..						
PG S_n	L	H	M	M	M	L

The following task is to calculate the particular criticality, stipulated by the given type of influence. We suggest using Bayesian belief networks (BBN) to evaluate the criticalities of the PG systems.

According to approach, it is suggested to construct BBN for each type of influence. Each node of BBN is represented by criticality matrix. Nodes are connected by links, which represent the different types of influence.

Hence, BBNs, which describe the PG system safety, consist of set of nodes. For each node the set of state is introduced. As mentioned, the state of node is characterized by a value of its criticality, calculated according to (2).

Every node also has a conditional probability table (CPT), associated with it. Conditional probabilities represent likelihoods based on prior information or past experience. A conditional probability is stated mathematically as, i.e. the probabilities of power grid system (child node) being at state characterized by expressions "Criticality is High (Medium, Low)", considering all possible combinations of other PG systems (parents' nodes) criticalities (High, Medium, Low).

As mentioned these conditional probabilities might be represented by linguistic values (for example High, Medium, Low).

Fragment of linguistic CPT is shown in the table 3.

Let's consider the fragment of BBN of S_1, S_2, S_3 represented on Fig.1, where criticality of S_3 (child node) is conditioned by criticalities both of S_2, S_3 (parents' nodes).

According to [13], probability of S_3, being at one of the established state Ω_{S3} depending on the states of parents nodes, could be determined as:

$$P(S_3^{(k)}) = \sum_i \sum_j P(S_3^{(k)} / S_1^{(i)},\ S_2^{(j)}) \times P(S_1^{(i)}) \times P(S_2^{(j)}) \quad (3)$$

Table 3

Fragment of CPT

S_1			S_2			S_3	
Criticality			Criticality			Criticality	
H	M	L	H	M	L	H	…
+			+			P(Crt(S_3)=H/Crt(S_1)=H, Crt(S_2)=H)=*High*	…
+				+		P(Crt(S_3)=H/Crt(S_1)=H, Crt(S_2)=M)=*Low*	…
						…….	..
	+		+			P(Crt(S_3)=H/Crt(S_1)=M, Crt(S_2)=H)=*Low*	…

where $P(S_3^{(k)})$ – a probability for S_3 being at *k*-th state; $P(S_3^{(k)}/S_1^{(i)}, S_2^{(j)})$ – a conditional probability for PG system S_3 to be at *k*-th state, provided system S_1 being at *i* th state and system S_2 being at *j* – th state; $P(S_1^{(i)})$ – probability for S_1 being at *i*-th state determined by expert, taking into account value (2); $P(S_2^{(j)})$ – probability for S_2 being at j-th state determined by expert, taking into account value (2).

Whereas linguistic BBN is used for PG safety analysis all probabilities in formula (5) are represented as linguistic variables.

Semantics of linguistic variables are supported by fuzzy sets. Fuzzy sets are obtained by the means of fuzzy arithmetic for triangular fuzzy numbers.

A triangular fuzzy number denoted by

$$M = <m, \alpha, \beta>,$$

has the membership function:

$$\mu_M(x) = \begin{cases} 0, \text{ for } x \le m - \alpha; \\ 1 - \dfrac{m - x}{\alpha}, \text{ for } m - \alpha < x < m; \\ 1 - \dfrac{x - m}{\beta}, \text{ for } m < x < m + \beta; \\ 0, \text{ for } x \ge m + \beta. \end{cases} \quad (6)$$

The point *m*, with membership grade of 1, is called the mean value and α, β are the left hand and right hand spread of M respectively.

If $M = <m, \alpha, \beta>$ and $N = <n, \gamma, \delta>$ are two TFNs then their addition is expressed as:

$$M \oplus N = <m + n, \alpha + \gamma, \beta + \delta>. \quad (7)$$

Multiplication $M \otimes N$ of two TFNs is not necessarily a triangular.

A good approximation is as follows:

$$M \otimes N = <m, \alpha, \beta> \otimes <n, \gamma, \delta> \cong <mn, m\gamma + n\alpha, m\delta + n\beta>. \quad (8)$$

Division of two TFNs is

$$\frac{M}{N} \cong \left\langle \frac{m}{n}, \frac{m\delta + n\alpha}{n^2}, \frac{m\gamma + n\beta}{n^2} \right\rangle. \quad (9)$$

These fuzzy arithmetic operations are used to calculate new linguistic probabilities represented by TFNs. These fuzzy probabilities usually do not match any linguistic term in the initial term set (High, Medium, Low), so a computing with words (CWW) procedure is needed to express there sult in the original expression domain.

The CWW is used to express the result in the original expression domain. CWW procedure uses the linguistic assessments and makes computations with them. Foundations and applications, providing the current status of theoretical and empirical developments in CWW, can be found in [14].

A linguistic aggregation operator based on the extension principle acts according to

$$S^n \xrightarrow{\tilde{F}} F(R) \xrightarrow{app_1(.)} S \quad (10)$$

where S^n symbolizes the n Cartesian product of S, $\tilde{F}$ is an aggregation operator based on extension principle, F(R) the set of fuzzy sets over the set of real number R, app_1: $F(R) \to S$ is a linguistic approximation function that returns a label from the linguistic term S, whose meaning is the closest to the obtained unlabeled fuzzy number, and S is the initial term set.

According to (5), the probabilities for system S_1, being at the state described by expression "Criticality - High", "Criticality – Medium" and "Criticality-High" might be calculated.

The power grid system S_i state, conditioned by the given type of influence, is determined on the criterion:

$$Crt(S_i) = \arg\max(P(Crt(S_i) = \text{High}), P(Crt(S_i) = \text{Medium}), P(Crt(S_i) = \text{Low})), \quad (11)$$

where $P(Crt(S_i) = \text{High})$ – a probability of power grid system of being at the state described by linguistic value High; $P(Crt(S_i) = \text{Medium})$ – probability of power grid system of being at the state described by linguistic value Medium; $P(Crt(S_i) = \text{Low})$ – probability of power grid system of being at the state described by linguistic value *Low*.

3. HPP accident case study based on linguistic Bayesian belief network

To demonstrate the approach to the power grid safety analysis, using the linguistic BBN, Russian Sayano–Shushenskaya HPP failure (August, 2009) is reviewed [15]. This HPP is one of the largest (together with Bratskaya HPP) one, used for power control of the whole power system with installed capacity - 6,4 mm kW, annual output - 22,8 bln kW p.h. Ten hydraulic units, each of 640 kW, are installed in the plant.

The BBN is built for fragment of Siberian power systems. BBN's nodes are criticalities matrixes of Sayano–Shushenskaya HPP– S_1, Mayansk HPP – S_2, Bratskaya HPP– S_3, Thermal Power Plant (TPP) of Bratsk – S_4.

Only physical influence is considered to evaluate state of $S_1$when conditional probabilities are expressed in linguistic values. Each node of Siberian power systems is completed by linguistic conditional probabilities table (see table 4).

The increasing of load from Bratskaya HPP and Mayansk HPP increased the criticality of S_1 and, finally, led to destruction of HPU – 2 (S_{32}). Increasing of criticality of S_1 led to increasing criticality of S_4.

Table 4

Fragment of Siberian power systems conditional probabilities table (before accident)

Mayansk HPP, S_1			Bratskaya, HPP S_2			Sayano–Shushenskaya HPP, S_3	
Criticality			Criticality			Criticality	
H	M	L	H	M	L	H	…
+			+			P(Crt(S_3)=H/Crt(S_1)=H, Crt(S_2)=H)=*High*	…
+				+		P(Crt(S_3)=H/Crt(S_1)=H, Crt(S_2)=M)=*High*	…
						…….	..
	+		+			P(Crt(S_3)=H/Crt(S_1)=M, Crt(S_2)=H)=*Low*	…

According to (5) the linguistic probabilities of S_3 being at the different states are calculated as:

$$P(Crt(S_3) = High)) = High;$$
$$P(Crt(S_3) = Medium)) = Low;$$
$$P(Crt(S_3) = Low)) = Low.$$

Considering (7) it is suggested that before Sayano–Shushenskaya HPP accident its criticality value might have been *High*.

Conclusions

Proposed technique may be applied to PG safety value prediction, taking into account its systems influence. The technique is based on the use of dynamical criticality matrices hierarchy. The power grid's capacity used to predict the possible safety change could be improved by implementing of the decision making system. The technique suggested in the paper is considered as a part of this system. PG safety assessment is carried out taking into consideration principles of dynamism, hierarchy, uncertainty and mutual influence of systems. BBN is used to predict the particular criticality of PG system, conditioned by the given type of influence. CWW is suggested to determine the probabilities of PG states expressed by linguistic values.

Results of analysis may be used to determine effective safety management strategies.

Consideration of the difference types of influence allows improving the accuracy of PG safety value.

Next step of technique enhancement will be related to consideration of Ukrainian NPP safety analysis, taking into consideration the types of influences of power grid and development of decision making tool-based system.

Aknowledgment

The presented paper has been conducted by V. Kharchenko within framework of the project "Integrating the National Aerospace University into ERA" (294311 KhAI-ERA, FP7-INCO-2011-16).

References

1 Linstone, H. Multiple Perspectives for Decision-Making: Bridging the Gap Between Analysis and Action [Text] / H. Linstone // North-Holland, Amsterdam, 1984. – P. 33 – 41.

2 Kaijser, A. The Swedish Infrastructure – Historical Development and Future Challenges [Text] / A. Kaijser // Carlsson, Stockholm, 1984. – 234 p.

3 Holmgren, A. Using Disturbance Data to Assess Vulnerability of Electric Power Delivery Systems [Text] / A. Holmgren, S. Molin // Journal Infrastructure systems, American Society of Civil Engineers (ASCE). – 2006. – Vol. 12, is. 4. – P. 243 – 251.

4 Bedford, T. Probabilistic Risk Analysis: Foundation and Methods [Text] / T. Bedford, R.M. Cooke // Cambridge University Press, Cambridge, England, 2001. – 166 p.

5 Hoyland, A. System Reliability Theory: Models and Statistical Methods [Text] / A. Hoyland, M. Rausald // Wiley, New York, USA, 1996. – P. 144 – 152.

6 Albert, R. Statistical Mechanics of Complex Networks [Text] / R. Albert, A.-L. Barabasi // Review of Modern Physics. – 2002. – Vol. 74. – P. 23 – 26.

7 Albert, R. Structural Vulnerability of North American Power Grid [Text] / R. Albert, I. Albert, G.L. Nakarado // Physical review E., 69, 025193 (R) (Rapid Communication), 2004. – P. 48 – 55.

8 Glass, R. Simulation and Analysis of Cascading Failure in Critical Infrastructure [Text] / R. Glass // Proceeding of Working Together: R&D Partnerships in Homeland Security, Boston. – April 2005. – P. 45 – 56.

9 Pan, H. Fuzzy Bayesian networks a general formalism for representation, inference and learning with hybrid Bayesian networks [Text] / H. Pan, L. Liu // IJPRAI. – 2000. – 14(7). – P. 941 – 962.

10 Komari, I.E. Extended Dependability Analysis of Information and Control Systems by FME(C)A-Technique: Models, Procedures, Application [Text] / I.E. Komari, V. Kharchenko, E. Babeshko // Proceedings of the Conference on Dependability of Computer

systems, Brunow, Poland, 30 June-02 July 2009, IEEE Computer Society. – Los Alamitos, California, 2009. – P. 25 – 32.

11 Brezhnev, E. Risk-analysis in critical information control system based on computing with words' model [Text] / E. Brezhnev // Proceeding of 7th International Workshop on Digital Technologies, Circuit Systems and Signal Processing, Zilina, Slovakia, 11-21 November. – 2010. – P. 67 – 72.

12 Bowles, J.B. An assessment of PRN prioritization in a failure modes effects and criticality analysis [Text] /J.B. Bowles // Journal of the IEST. – 2004. – Vol. 47, N: 51-6. – P. 74 – 81.

13 On-line Tutorial on Bayesian nets and probability [Electronic resource]. – Access mode: http://www.dcs.qmw.ac.uk/%7Enorman/BBNs/BBNs.htm. – 15.01.2012 y.

14 Zadeh, L. Computing with words in Information [Text] / L. Zadeh, J. Kacprzyk // Intelligent Systems. – Part 1: Foundation; Part 2. – USA, 2001. – P. 14.15 – 14.21.

15 Causes of destruction of Sayano–Shushenskaya HPP hydraulic unit 2 [Electronic resource]. – Access mode: http://zhurnal.lib.ru/b/boris_i_k/prichinyrazrus–chenijagidroagregata2sschges.shtml. – 15.01.2012 y.

Поступила в редакцию 23.02.2012

Рецензент: д-р техн. наук, проф. В.А. Твердохлебов, Институт проблем точной механики и управления РАН, Саратов, Россия

ОЦЕНКА БЕЗОПАСНОСТИ ЭНЕРГОСИСТЕМЫ С ИСПОЛЬЗОВАНИЕМ ЛИНГВИСТИЧЕСКОЙ БАЙЕСОВСКОЙ СЕТИ ДОВЕРИЯ

Е.В. Брежнев, В.С. Харченко

Безопасность энергосистемы определяется состоянием ее подсистем, обусловленных в свою очередь их взаимным влиянием различной природы. Изменение этого влияния приводит к изменению состояний подсистем, и как следствие, к изменению безопасности энергосистемы на протяжении всего ее жизненного цикла. Предложенный подход основан на применении байесовской сети доверия, в которой узлы представляют различные подсистемы, а связи обусловлены взаимным влиянием между ними. Рассматриваются различные типы влияния между подсистемами (физическое, информационное, географическое, и т.д.). В качестве показателя безопасности энергосистемы предлагается использовать оценку критичности. Критичность и влияние рассматривается как лингвистические переменные. Предлагается оценивать критичность энергосистемы с учетом изменений состояний ее подсистем. Условные вероятности также оцениваются как лингвистические переменные. В качестве примера предлагаемого подхода рассматривается авария, произошедшая на Саяно-Шушенской гидроэлектростанции.

Ключевые слова: Энергосистема, лингвистические вычисления, безопасность, байесовская сеть доверия

ОЦІНКА БЕЗПЕКИ ЄНЕРГОСИСТЕМИ З ВИКОРИСТАННЯМ ЛІНГВІСТИЧНОЇ БАЙЕСОВСЬКОЇ МЕРЕЖИ ДОВІРИ

Є.В. Брежнєв, В.С. Харченко

Безпека енергосистеми визначається станом її підсистем, які в свою чергу обумовлені взаємним впливом різної природи. Зміна цього впливу призводить до зміни станів підсистем, та як наслідок, обумовлює зміну безпеки енергосистеми протягом її життєвого циклу. Підхід, який запропоновано, ґрунтується на використанні байесовської мережі довіри, в якій вузли представлені підсистеми, а зв'язки обумовлені взаємним впливом між ними. Розглядаються різні типи впливів між підсистемами (фізичний, інформаційний, географічний, та інш.). В якості показника безпеки енергосистеми пропонується оцінка критичності. Критичність та вплив розглядаються як лінгвістичні змінні. Пропонується оцінювати критичність енергосистеми з урахуванням зміни станів її підсистем. Умовні імовірності також оцінюються як лінгвістичні змінні. В якості прикладу застосування підходу розглядається аварія на Саяно-Шушенській гідроелектростанції.

Ключові слова: Енергосистема, лінгвістичні обчислення, безпека, байєсівська мережа довіри

Brezhnev Eugene – PhD, Doctor of Science student of the Computer System and Network Department, National Aerospace University, Kharkiv, Ukraine.

Kharchenko Vyacheslav – Professor, Doctor of Science, Head of Computer Systems and Networks Department, National Airspace University "KhAI" and Centre of Safety Infrastructure-Oriented Research and Analysis, Ukraine.