Advances in Intelligent Systems Research, volume 169
VIth International Workshop 'Critical Infrastructures: Contingency Management, Intelligent, Agent-Based, Cloud Computing and Cyber Security' (IWCI 2019)

Fractal Stratified Model Development for Critical Infrastructure from the standpoint of Energy and Cyber Security

Daria Gaskova
Melentiev Energy Systems Institute of
Siberian Branch of the Russian Academy of Sciences
Irkutsk, Russia
gaskovada@gmail.com

***Abstract*— The article discusses the research model of the energy sector as one of the main critical infrastructures from the point of view of energy security and the inclusion of cyber security issues. The model is built upon the fractal approach which allows one to represent a subject field as a set of information layers and their mappings from any layer into each one. The description of the model and how it is used in the Intelligent System for cyber threat analysis and risk assessment of cyber security violation at energy facilities results in this article.**

***Keywords*— fractal approach, energy infrastructure, semantic modeling methods, energy security, cyber threats**

I. INTRODUCTION

The article considers energy sector as a specific critical infrastructure. The state program "Digital Economy" is currently being implemented in Russia, under which the tendency of the digital transformation of the energy sector is observed [1]. New information and communication technologies in complex technological systems are usually applied through the introduction of advanced technological solutions and new business models, that could be accompanied by occurrence new risks.

Security issues of complex technological systems lie in the area of risk management [2] and systems-based risk analysis [3]. Haimes Y. proposed Hierarchical Holographic Modeling (HHM) [4] for systems-based risk analysis of large-scale systems. The HHM scheme integrates several models and represents various aspects of the system in terms of its organizational and functional structures, the various time horizons, multiple decision makers, stakeholders and users of the system, and other socio-economic conditions that need to be considered. Synthesis of identified risks from different points of view could then give a more complete picture of the overall systemic risk [4].

The work devotes to the study of the energy sector, which is one of the main critical infrastructures [5], taking into account the aspects of cyber and energy security. The issues under consideration use a similar approach, but a broader one to knowledge structuring. The integration of methods, models and basic concepts of the subject fields is made on the basis of the fractal approach.

Energy facilities provided with modern equipment could be considered as a cyber-physical system [6, 7]. Issues of influence from the IT infrastructure on the physical infrastructure lie in the field of cyber security research. The present work reviews the energy sector as critical infrastructures, in which extreme situations could arise due to cyber threats realization.

Methods of system analysis and semantic modeling are proposed to study the area of concern. Such methods enable to identify the main concepts and their interrelations, to determine the main stages of the study, and to carry out a preliminary qualitative assessment under conditions of lack or incompleteness of statistical data.

II. FRACTAL APPROACH

The fractal approach is proposed by D.Sc. in Engineering L.V. Massel in the nineties of the last century. The approach is to build a fractal stratified model (FS model) to knowledge structuring. FS model is based on the representation of different forms of knowledge as information objects of a stratified space [8].

FS-model is defined as a set of crossing-free layers or information worlds and their mappings in information space. Each level of knowledge representation is a layer of this space and corresponds to its information world. The sequence of mappings reflects the process of knowledge. FS model can be graphically displayed as a set of nested spheres. The information object is a point on one of the spheres. When ones are required to consider in detail such objects it is carried out by its stratification, and other objects can also be considered "pointwise" at that. Therefore, the fractal approach allows us to work with multi-scale objects using the same methods, keeping an invariant of the object (its existing properties) when one going from layer to layer in doing so mapping.

The mathematical description of the FS model is given in [9]. A researcher knowledge on a certain issue is presented as a portion of the information space, which is called a "fractal" within the fractal approach. It graphically represents a cone or pyramid, which includes some layers. Such a cone can be a discipline, approach or method.

The application of the fractal approach to semantic modeling in the energy sector is described in [10].

Applying the fractal approach for semantic modeling allows one to easily consider a point of interest, avoiding models of large dimension, which usually include a large number of concepts and relationships that make it more complex to be understood while fully represented. The fractal approach permits to detail or to aggregate concepts while retaining the internal structure of relationships and meaning, and also provides the possibility of a multi-scale presentation of semantic models [10].

A. *Fractal approach to design information technology*

The application of the fractal approach to design information technology is considered in [11]. A traditional problem-solving sequence includes task, model, algorithm, program, data, and software product. Ones could allocate the basic layers in accordance with this sequence for the field of information technologies. In this case, there are mathematical models layer, algorithms layer, programs layer, data models layer, knowledge models layer.

We can represent any information technology as a set of information layers and their mappings by the use of the fractal approach. The designing of information technology is to develop ways to describe information layers or objects and ways of mapping from any layer to each one in this case. Meanwhile, instrumental tools to support specific information technology provide the implementation of these methods.

The fractal approach to the design of information systems architecture is considered in [12]. Within this approach, the typical stratification of information systems is the separation of three levels: 1) the data management level, 2) the level of applied logic (business logic) and 3) the interface management level.

There are three phases of precomputer designing knowledge-based systems within knowledge engineering, which are described in [13]:

1) *knowledge acquiring phase,* the result of which is a huge number of conflicting pieces of knowledge;

2) *knowledge structuring phase,* as a result of which the fragmented pieces of knowledge are aggregated into a single model, called the knowledge field;

3) *knowledge field formalization phase* using specialized knowledge representation languages, the result of which is a knowledge base.

The paper presents the FS model as the result of the second phase of knowledge engineering. We can then formulate research techniques and design intelligent system on the basis of such the model.

III. Fractal Stratified Model of Knowledge Space about Critical Infrastructure from the Standpoint of Energy and Cyber Security.

Within the fractal approach to data and knowledge structuring one could perform a stratification of the data and knowledge space *D* and build mappings from any layer into each one. Therefore, the information space of data and knowledge for cyber threat analysis and risk assessment of cyber security violation at energy facilities is described as (1):

$$D = \{D_M, D_E, D_V, D_T, D_R\}, \qquad (1)$$

where D_M is the proposed methods layer; D_E is the energy infrastructure layer; D_V is the vulnerabilities layer; D_T means the threats layer, D_R is the risks layer.

Fig. 1 shows the FS model describing the relationships of the proposed methods, energy infrastructure, vulnerabilities, threats, and risks.

The presented FS model includes six types of mappings *F*:

- $F_M^E: D_M \to D_E$ means mapping from the methods layer to the energy infrastructure layer;
- $F_M^V: D_M \to D_V$ denotes mapping from the methods layer to the vulnerabilities layer;
- $F_M^T: D_M \to D_T$ signifies mapping from the methods layer to the threats layer;
- $F_E^V: D_E \to D_V$ indicates mapping from the energy infrastructure layer to the vulnerability layer;
- $F_V^T: D_V \to D_T$ stands for mapping from the vulnerabilities layer to the threats layer;
- $F_T^R: D_T \to D_R$ designates mapping from the threats layer to the risks layer.

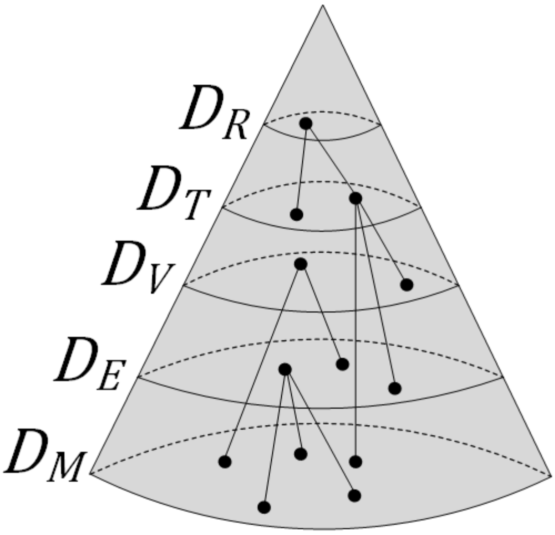

Fig. 1. The FS model describing the relationships of the proposed methods, energy infrastructure, vulnerabilities, threats, and risks

Further, we could represent the methods layer as (2):

$$D_M = \{O, ExS, B, Rm\}, \qquad (2)$$

where *O* is the ontological engineering methods layer; *ExS* means the expert systems technology layer; *B* is the Bayesian Belief Network (BBN) layer; *Rm* is the methods layer for systems analysis of risk.

The energy infrastructure layer looks like (3):

$$D_E = \{E_t, E_s, E_o\}, \qquad (3)$$

where E_t is the layer of the energy sector level; E_s is the layer of energy systems level; E_o means the layer of energy facilities (EF) level.

The vulnerabilities layer is introduced by (4):

$$D_V = \{V_c, V_e, V_{ex}\}, \qquad (4)$$

where V_c is the layer of IT infrastructure vulnerabilities; V_e is the layer of industrial equipment vulnerabilities; V_{ex} means the layer of external vulnerabilities.

The threats layer consists of the next parts (5):

$$D_T = \{T_c, T_e, T_{ex}\}, \qquad (5)$$

where T_c is the cyber threats layer; T_e is the layer of threats to energy security; T_{ex} is the layer of external threats.

The risk layer is represented by (6):

$$D_R = \{R_i, R_a\}, \qquad (6)$$

where R_i is the IT infrastructure risk layer; R_a is the risk layer of accidents and catastrophes.

Fig. 2 illustrates the layers and their mappings of information space *D*. Constructing the FS model permitted to determine the follows stages of the study:

- analysis of energy facility assets;
- analysis of the vulnerabilities of the energy facility assets;
- analysis of cyber threats and threats to energy security at an energy facility;
- risk assessment of the occurrence of an extreme situation caused by the implementation of cyber threats.

The FS model can be interpreted as follows. The analysis of EF assets corresponds to the mapping F_M^E from the proposed methods layer to the energy infrastructure layer. The analysis of the vulnerabilities of EF assets corresponds to the mapping F_M^V from the proposed methods layer to the vulnerabilities layer and mapping F_E^V from the energy infrastructure layer to the vulnerabilities layer. The cyber threats analysis of EF corresponds to the mapping F_M^T from the proposed methods layer to the threats layer and the mapping F_V^T from the vulnerabilities layer to the threats layer. The risk assessment of the occurrence of an extreme situation in the energy sector, caused by cyber threats, corresponds to the mapping F_T^R from the threats layer to the risks layer.

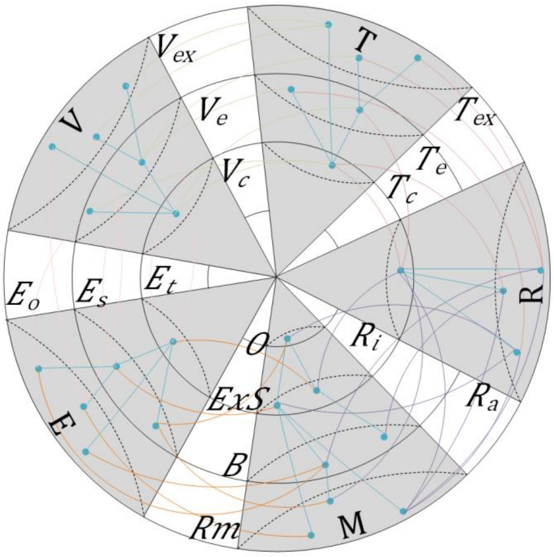

Fig. 2. Extended FS model of energy infrastructure from the perspective of cyber and energy security

A. The FS-model application when developing the Intelligent System

The Intelligent System for cyber threat analysis and risk assessment of cyber security violation at energy facilities is being developed within the study of the cyber threats impact on extreme situation initiation in the energy sector.

Intelligent System [14] includes a set of three main components: 1) the production expert system for identifying the vulnerabilities of the information and communication system and the corresponding cyber threats; 2) the unit of BBN for probabilistic modeling of extreme situations at energy facilities caused by the implementation of cyber threats; 3) and the unit to assess risk from violation of cyber and energy security.

The object-oriented methodology [15] uses to analysing and designing complex systems for various purposes and provides the basis for a semantic model is designed using considered FS model.

The Class Diagram in the UML notation is employed to develop a semantic model and it is presented in Fig. 3. Classes are described in Java. Each layer of the FS model could be represented by a set of classes and their internal variables. Some inheriting classes form a hierarchy, which delivers a representing the cone structure of the presented FS model. Class methods support mapping from layer to layer.

The use of the FS model in building the Intelligent System contributes to [11]:

- conceptually integrate different ways of knowledge structuring, applied in various considered areas of knowledge, which are

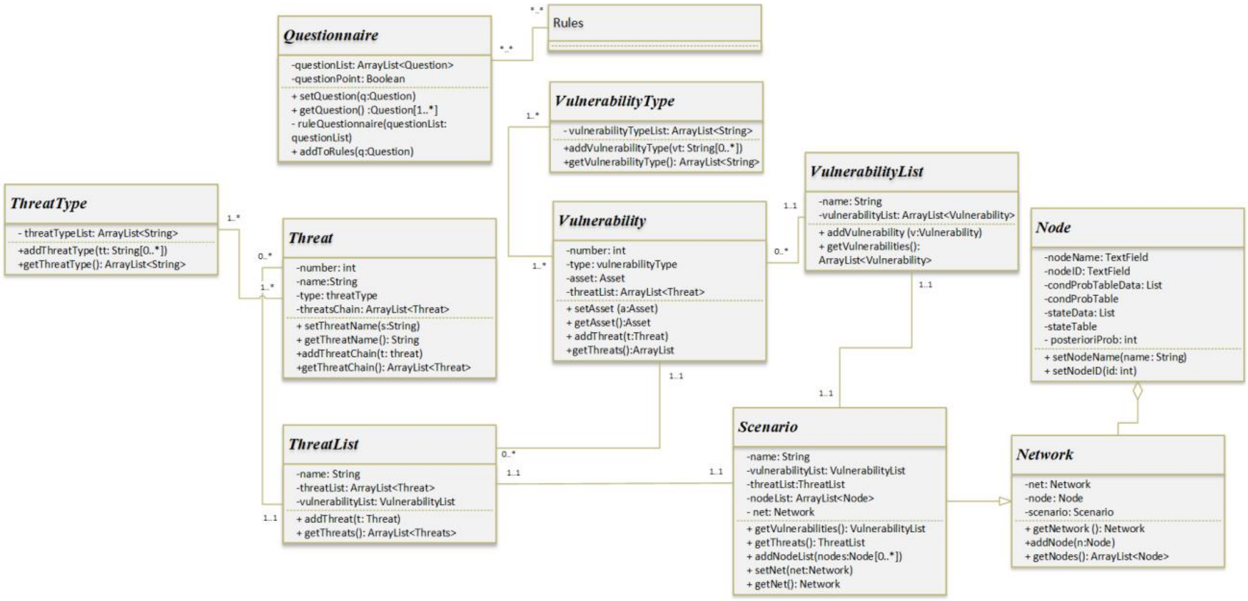
Questionnaire
-questionList: ArrayList<Question>
-questionPoint: Boolean
+ setQuestion(q:Question)
+ getQuestion() :Question[1..*]
- ruleQuestionnaire(questionList: questionList)
+ addToRules(q:Question)
Rules
..
..
VulnerabilityType
- vulnerabilityTypeList: ArrayList<String>
+addVulnerabilityType(vt: String[0..*])
+getVulnerabilityType(): ArrayList<String>
1..*
ThreatType
- threatTypeList: ArrayList<String>
+addThreatType(tt: String[0..*])
+getThreatType(): ArrayList<String>
1..*
0..*
1..*
Threat
-number: int
-name:String
-type: threatType
-threatsChain: ArrayList<Threat>
+ setThreatName(s:String)
+ getThreatName(): String
+addThreatChain(t: threat)
+getThreatChain(): ArrayList<Threat>
1..*
Vulnerability
-number: int
-type: vulnerabilityType
-asset: Asset
-threatList: ArrayList<Threat>
+ setAsset (a:Asset)
+ getAsset():Asset
+ addThreat(t:Threat)
+getThreats():ArrayList
1..1
0..*
VulnerabilityList
-name: String
-vulnerabilityList: ArrayList<Vulnerability>
+ addVulnerability (v:Vulnerability)
+ getVulnerabilities(): ArrayList<Vulnerability>
1..1
Node
-nodeName: TextField
-nodeID: TextField
-condProbTableData: List
-condProbTable
-stateData: List
-stateTable
- posterioriProb: int
+ setNodeName(name: String)
+ setNodeID(id: int)
1..1
1..1
ThreatList
-name: String
-threatList: ArrayList<Threat>
-vulnerabilityList: VulnerabilityList
+ addThreat(t: Threat)
+ getThreats(): ArrayList<Threats>
0..*
1..1
1..1
1..1
Scenario
-name: String
-vulnerabilityList: VulnerabilityList
-threatList:ThreatList
-nodeList: ArrayList<Node>
- net: Network
+ getVulnerabilities(): VulnerabilityList
+ getThreats(): ThreatList
+ addNodeList(nodes:Node[0..*])
+ setNet(net:Network)
+ getNet(): Network
Network
-net: Network
-node: Node
-scenario: Scenario
+ getNetwork (): Network
+addNode(n:Node)
+ getNodes(): ArrayList<Node>

Fig. 3. Fragment of a Class Diagram in UML notation

necessary for cyber threat analysis and risk assessment of cyber security violation at energy facilities;

- apply various methods of isolating and ordering layers depending on the use case of the system;
- focus on the current layers that are the subject of the study, paying tribute to the significance of other layers;
- ensure the consistent implementation of the strategy of building the Intelligent System, which is achieved by introducing an invariant, regardless of the depth of separation of individual worlds.

IV. Conclusions

The presented FS model displays an expanded data and knowledge structure in the zone of intersection of energy and cyber security areas and also includes the proposed research methods for each of the layers. There are three advantages to building the FS model in the study. Firstly, the ability to isolate basic data and knowledge about critical infrastructure from the perspective of energy and cyber security. Some of such terms are vulnerabilities, threats and risks in the context of current trends in the development of the energy sector and interrelations with existing problems of energy security. Secondly, the use of the FS model allows one to operate with data and knowledge of varying detail degrees with the ability to preserve the overall structure of relationships and meaning, as well as to combine different subject areas in the form of a portion of information space, which is represented as a cone. Thirdly, this approach of knowledge formalization could allow achieving the necessary abstraction level, which, on the one hand, permits one to operate with the available data and knowledge when building various models, and on the other, to determine the main interrelations between the objects of information layers of the research field. Apart from that, the research field is characterized by rather high variability and the rate of appearance of new vulnerabilities, threats and methods for their implementation. In turn, the use of related methods and the construction of a set of partial models based on the FS model will allow determining the final assessment of the consequences of the cyber threats implementation in the energy sector.

Acknowledgment

This work was performed within the framework of project according to state assignment ESI SB RAS №AAAA-A17-117030310444-2. The studying of separated aspects was supported by RFBR grants № 19-07-00351, № 19-57-04003, № 18-07-00714, № 18-37-00271, № 17-07-01341.

References

[1] L.V Massel, "Methods and Intelligent Technologies for Scientific Substantiation of Strategic Solutions on Digital Transformation of Energy Industry," in Energy Policy No. 5, 2018, pp. 30-42 ["Metody i intellektual'nye tekhnologii nauchnogo obosnovaniya strategichskih reshenij po cifrovoj transformacii energetiki," Energeticheskaya politika, No. 5, 2018, pp. 30-42] (In Russian).

[2] N.A Mahutov, N.V. Abrosimov, M.M. Gadenin, "Security Enforcement is a Priority in Basic and Applied Research," in Economic and social changes: facts, trends, forecast, No. 3(27), 2013, pp. 46-71 ["Obespechenie bezopasnosti – prioritetnoe napravlenie v oblasti fundamental'nyh i prikladnyh issledovanij," Ekonomicheskie i social'nye peremeny: fakty, tendencii, prognoz No. 3(27), 2013, pp. 46-71] (In Russian).

[3] Y.Y. Haimes,"Systems-based risk analysis," in Global Catastrpphic Risks, Nick Bostrom, Milan M. Cirkovic (ed), Oxford, 2008, pp. 146-163.

[4] Y.Y. Haimes, J. Lambert, L. Duan, R. Schooff, and V. Tulsiani, "Hierarchical holographic modeling for risk identification in complex systems,"1995 IEEE International Conference on Systems, Man and Cybernetics. Intelligent Systems for the 21st Century, pp.1027-1032.

[5] A. Kondratev, “The Current Trends in Research of Critical Infrastructure in Foreign Countries,” in Foreign Military Review. No. 1, 2012, pp. 19-30 [“Sovremennye tendencii v issledovanii kriticheskoj infrastruktury v zarubezhnyh stranah,” Zarubezhnoe voennoe obozrenie, No. 1, 2012, pp. 19-30] (in Russian).

[6] L.V. Massel, A.G. Massel, “Semiotic Approach to the Creation of Intelligent Situational Ccontrol Systems in the Energy Sector,” in Proceedings of the XLIII International conference “Information technology in science, education and management”, Moscow, Russia, 2015, pp. 182-193 [“Semioticheskij podhod k sozdaniyu intellektual'nyh sistem situacionnogo upravleniya v energetike,” in Trudy XLIII Mezhdunarodnoj konferencii “Informacionnye tekhnologii v nauke, obrazovanii i upravlenii”, Moscow, Russia, 2015, pp. 182-193] (In Russian).

[7] E. Zio, “Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures,” in Reliability Engineering and System Safety, vol. 152, 2016, pp. 137–150.

[8] L.V Massel, “Fractal Approach to Knowledge Structuring and Examples of its Application,” in Ontology of designing. vol.6, No. 2 (20), 2016; pp. 149-161 [“Fraktal'nyj podhod k strukturirovaniyu znanij i primery ego primeneniya,” Ontologiya proektirovaniya, vol.6, No. 2 (20), 2016; pp. 149-161] (in Russian).

[9] L.V Massel, “Fractal Model of Knowledge Structuring,” in Proceedings of the National conference with international participation “AI-94”, Rybinsk, Russia, 1994, Vol. 1, pp. 46-49 [“Fraktal'naya model' strukturirovaniya znanij,” in Sbornik nauchnyh trudov Nacional'noj konferencii s mezhdunarodnym uchastiem “Iskusstvennyj intellekt-94”, Rybinsk, Russia, 1994, Vol. 1, pp. 46-49] (in Russian).

[10] A.G. Massel, “Fractal approach to semantic modeling,” in Proceedings of the 5 th All-Russian Conference on Information Technologies for Intelligent Decision Making Support “ITIDS2017”, Ufa, Russia, 2017, pp. 15-19 [“Fraktal'nyj podhod k semanticheskomu modelirovaniyu,” in Trudy pyatoj vserossijskoj konferencii “Informacionnye tekhnologii intellektual'noj podderzhki prinyatiya reshenij”, Ufa, Russia, 2017, pp. 15-19] (in Russian).

[11] L.V Massel, “Fractal Approach to the Construction of Information Technologies,” in Information technology of energy development research, Novosibirsk: Nauka, 1995, pp. 40-67 [“Fraktal'nyj podhod k postroeniyu informacionnyh tekhnologij,” in Informacionnaya tekhnologiya issledovanij razvitiya energetiki, Novosibirsk: Nauka, 1995, pp. 40-67] (in Russian).

[12] A.N. Kopaygorodsky, L.V. Massel, “Fractal Approach to Designing the Architecture of Information Systems,” in Proceedings of Irkutsk State Technical University, No. 6 (46), 2010, pp.8-12.

[13] T.A. Gavrilova, D.V. Kudryavcev, and D.I. Muromcev, Knowledge Engineering. Models and methods, SPb: Lan publishing house, 2016, 324 p [“Inzheneriya znanij. Modeli i metody,” SPb: Lan’, 2016, 324 p] (in Russian).

[14] A.G. Massel, D.A. Gaskova, “Scenario Approach for Analyzing Extreme Situations in Energy from a Cybersecurity Perspective,” in Industry 4.0, 2018, Issue 5. Publisher: Scientific Technical Union of Mechanical Engineering “Industry 4.0”, pp. 266-269.

[15] V.A. Silich, M.P. Silich, Theory of Systems and System Analysis, Tomsk: Tomsk Polytechnic University, 2011, 278 p