Vulnerability Analysis of Intelligent Integrated Energy Systems

Evgeny Barakhtenko
Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, ESI SB RAS
Irkutsk, Russia
barakhtenko@isem.irk.ru

Dmitry Sokolov
Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, ESI SB RAS
Irkutsk, Russia
sokolov_dv@isem.irk.ru

Alexei Edelev
Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences, ESI SB RAS
Irkutsk, Russia
flower@isem.irk.ru

Sergei Gorsky
Matrosov Institute for System Dynamics and Control Theory of the Russian Academy of Sciences, IDSTU SB RAS
Irkutsk, Russia
gorsky@icc.ru

***Abstract*—The paper addresses the intelligent integrated energy systems vulnerability analysis framework. The main task of intelligent integrated energy systems similar to any energy supply system is the consumer's uninterruptable energy supply. This paper describes the main principles to deal with the complexity of intelligent integrated energy systems when performing their vulnerability analysis. The engineering-based framework suitable for vulnerability analysis of intelligent integrated energy systems is proposed.**

Keywords*— *intelligent integrated energy systems, modeling, vulnerability analysis, distributed computing

I. Introduction

The appearance of new technologies and equipment, new requirements for energy supply systems and change of the their functionality conditions make eventually more important the transition to integrated supply systems which are the combination of power, heat, cold and gas supply systems [1]. The main task of intelligent integrated energy systems (IIES) similar to any energy supply system is the uninterruptable energy supply of consumers. This task becomes especially important under emergency conditions.

Emergencies include natural disasters such as floods, storms, etc., and technical hazards, such as failures. The both types of emergencies by nature are large disturbances that negatively affect the resilience of IIES considered as a system of interconnected critical infrastructures. The resilience here is understood as the ability of critical infrastructures to prevent damage before disturbance events, mitigate losses during the events and improve the recovery capability after the events [2]. Fig. 1 illustrates the resilience concept [3]. The system performance function φ(t) is measured before, during, and after a disturbance. A system operates in the stable original state until a disturbance occurs at te, and at time td the system reaches its maximum disrupted state. The system recovery starts at time ts, and stable recovered state is achieved at time tf and is maintained after.

Two dimensions of resilience, vulnerability, and recoverability, are shown in Fig. 1. The last refers to the speed of the system recovery after a disturbance while the former expresses the consequences value of a disturbance impact on a system.

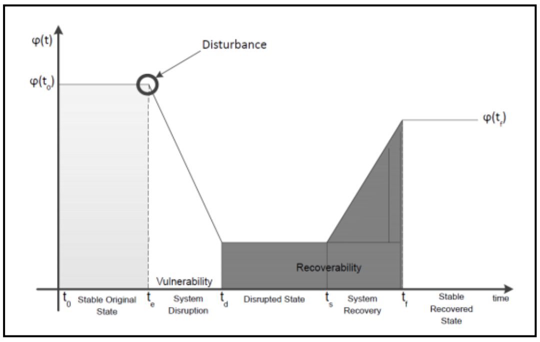

Figure 1. The performance of a system, ϕ(t), before, during, and after a disturbance. Adopted from [3].

II. The Complexity of Intelligent Integrated Energy Systems

IIES are complex system organized in a hierarchy of physically and functionally heterogeneous subsystems. The hierarchy includes different types of energy (power, heat, gas, etc.) supply systems and a telecommunication system. This leads to both structural and dynamic complexity of IIES [4].

Each supply subsystem of IIES consists of a specific set of components. The components can be divided into the following groups according to their energy functionality: generation, transmission, distribution, and consumption. In turn, each component is associated with a particular set of equipment representing its energy functionality and type of the IIES subsystem that includes it.

The IIES complexity implies to take into account the following important characteristics of IIES for their vulnerability analysis:

- Interaction of different energy supply systems,
- Intelligence property,
- Different consequences of an emergency impact on particular subsystems.

The first characteristic provides the mutual reservation of the energy supply systems constituted the IIES. In case of an emergency, it is possible to ensure energy resource and source diversification that causes energy flow redistribution in the IIES subsystems and thus enables finding the ways of emergencies mitigation or their negative impact reduction.

The second characteristic gives to IIES an ability to forecast, assess and adapt to the different internal and external conditions. The intelligent software, variety of sensors, and secure communication channels permit the fast restoration of energy supply after emergencies occurrence and minimizing their impact [5]. Also involving smart technologies such as energy storage, demand response with flexible loads in energy infrastructure models would be a future trend [6].

III. System-of-Systems Conception

To deal with the IIES complexity in their vulnerability analysis the IIES have to be seen based on the “system-of-systems” conception [7, 8]. The system-of-systems “consist of multiple, heterogeneous, distributed, occasionally independently operating systems embedded in networks at multiple levels that evolve over time” [9]. The system-of-systems conception supposes the multi-hierarchical model architecture. There are two main alternative implementations: integrated approach and coupled approach [8]. An integrated model covers all hierarchical levels and contains detailed low-level models of subsystems as well as a high-level model. A coupled model aggregates outputs of the low-level models as inputs at a higher level.

IV. Critical Infrastructures Integration

Besides system-of-systems conception the comprehensive consideration of critical infrastructures interdependencies [10] is a key to successful vulnerability analysis of the IIES. A number of different definitions for interdependency have been proposed in the literature [11-15]. One of the more commonly using frameworks for characterization is the one proposed by Rinaldi et al. [11], where interdependencies are grouped into four categories:

- Physical (functionality of each infrastructure depends on the material or physical outputs of the other),
- Cyber (each infrastructure depends on information transfer from the other),
- Geographical or spatial (a single local disruptive event can cause state changes in geographically interdependent infrastructures), and
- Logical (dependencies other than the above three categories).

It should be noted that the field of critical infrastructures integration and interdependencies is still quite immature and is better investigated on the urban, rural, or regional scales rather than on the national level [6].

V. Approaches for Interdependent Critical Infrastructures Modeling

There exist many approaches for modeling interdependent critical infrastructures and they can be broadly categorized into six types [7]: empirical approaches, agent-based approaches, system dynamics based approaches, economic theory based approaches, network-based approaches, and others.

The network-based approaches suitable for modeling IIES can be divided into the following categories [16]:

- Network-based models describing the system behavior strictly on pure topological properties,
- Network-based models studying the functional properties by computing the flow of resources or services in the system,
- Engineering-based approaches utilizing the physical laws that manage the flows in different infrastructures.

VI. Subject-Oriented Environment

The IIES vulnerability analysis can be performed using different computing systems (personal computer, server, cluster, grid, or cloud) for a relatively acceptable time (hours, days), the duration of which is determined by the characteristics of the used computing resources. Integration of the listed systems into a single environment provides both the flexibility in choosing the necessary configuration of the computational infrastructure and speed in implementing experiments of various scales [17]. We use a modular approach when developing applications that operate in such an environment [14]. This environment ensures the possibility of an integration of modules of existing applications for solving various energy problems (for example, [19-21]) when applied software for solving new challenges is developed. The special system for meta-monitoring environment resources provides the high reliability of distributed computing [22].

VII. The Engineering-Based Framework Suitable for Vulnerability Analysis of Intelligent Integrated Energy Systems

Taking into account the structural and dynamic complexity of the IIES, the characterization of the hazards and the evaluation of their social and technical consequences according to [4] there is no single modeling approach that captures all features of IIES vulnerability.

A vulnerability analysis framework to integrate a number of existing methods and new analysis approaches capable of viewing the interdependent critical infrastructures complexity problem from topological, functional and other perspectives proposed in [23]. In the [23] interdependencies are classified as either functional (including physical, cyber and logical interdependencies from the classification proposed by Rinaldi et al. [11], since these can be treated in the same basic way) or geographical (from the classification proposed by Rinaldi et al. [11]).

The engineering-based approach [17] suitable for vulnerability analysis of IIES was developed on the base of [19] and provides one unified way of modeling systems to represent critical infrastructures of different types. It is oriented to use resources of public access computer center "Irkutsk Supercomputer Center of SB RAS [24]. The built models are merged into one system-of-systems model to incorporate the effects of critical infrastructure interdependencies. Together it enables solving new problems of the comprehensive vulnerability analysis of energy critical infrastructures based on a single system modeling approach taking into account higher order interdependencies between them. In addition, this approach provides a possibility to choose functional models that correspond to both the specific energy critical infrastructures and the domain of particular research.

VIII. CONCLUSIONS

IIES are considered critical infrastructures because their inoperability or destruction has a significant impact on the society, state, and economy. IIES are complex system organized in a hierarchy of physically and functionally heterogeneous subsystems. They consist of different types of energy supply systems and the telecommunication system. This leads to both structural and dynamic complexity.

There are some ideas to deal with complexity for IIES vulnerability analysis:

- Usage of system-of-systems conception to represent IIES structure,
- Comprehensive consideration of IIES interdependencies,
- Utilization of network-based methods for modeling IIES,
- Developing a subject-oriented environment for rapid computations.

On the basis of the ideas above, the paper addresses the engineering-based framework suitable for IIES vulnerability analysis.

ACKNOWLEDGMENT

The work was carried out within framework of scientific projects III.17.4.1 (No. AAAA-A17-117030310432-9), III.17.5.1 (No. AAAA-A17-117030310451-0), and IV.38.1.1 (AAAA-A17-117032210078-4) of the program of fundamental research of the Siberian Branch of the Russian Academy of Sciences. It was also supported in part by the Russian Foundation of Basic Research, project no. 19-07-00097-a.

REFERENCES

[1] N. I. Voropai, V. A. Stennikov, and E. A. Barakhtenko, “Methodological principles of constructing the integrated energy supply systems and their technological architecture,” in Journal of Physics: Conference Series, vol. 1111, no. 1, p. 012001, December 2018.

[2] G. Sansavini, “Engineering resilience in critical infrastructures,” in Resilience and Risk. NATO Science for Peace and Security Series C: Environmental Security, pp. 189-203, 2017.

[3] Y. Almoghathawi, K. Barker, and L. A. Albert, “Resilience-driven restoration model for interdependent infrastructure networks,” in Reliability Engineering & System Safety, vol. 185, pp.12-23, 2019.

[4] E. Zio, “Challenges in the vulnerability and risk analysis of critical infrastructures,” in Reliability Engineering and System Safety, vol. 152, pp. 137-150, 2016.

[5] M. Amin, “Toward self-healing energy infrastructure systems,” in IEEE Computer Applications in Power, vol. 14, no. 1, pp. 20-28, January 2001.

[6] J. Wang, W. Zuo, L. Rhode-Barbarigos, X. Lu, J. Wang, and Y. Lin, “Literature review on modeling and simulation of energy infrastructures from a resilience perspective,” in Reliability Engineering & System Safety, vol. 183, pp. 360-373, 2019.

[7] M. Ouyang, “Review on modeling and simulation of interdependent critical infrastructure systems,” in Reliability engineering & System safety, vol. 121, pp. 43-60, 2014.

[8] I. Eusgeld, C. Nan, and S. Dietz, “System-of-systems” approach for interdependent critical infrastructures,” in Reliability Engineering & System Safety, vol. 96, no. 6, pp.679-686, 2011.

[9] D. DeLaurentis, “Role of humans in complexity of a system-of-systems,” in Lecture Notes in Computer Science, vol. 4561, pp. 363-371, 2007.

[10] S. Saidi, L. Kattan, P. Jayasinghe, P. Hettiaratchi, and J. Taron, “Integrated Infrastructure Systems – A Review,” in Sustainable Cities and Society, vol. 36, pp. 1-11, 2018.

[11] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, “Identifying, understanding, and analyzing critical infrastructure interdependencies,” in IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11-25, December 2001.

[12] E. E. Lee, J. E. Mitchell, and W.A. Wallace, “Restoration of services in interdependent infrastructure systems: a network flows approach,” in IEEE Trans. Syst. Man. Cybern. Part C: Appl Rev, vol. 37(6), pp. 1303–17, 2007.

[13] R. Zimmerman, “Social implications of infrastructure network interactions,” in J. Urban Technol., vol.8, pp. 97–119, 2001.

[14] D. D. Dudenhoeffer, M. R. Permann, and M. Manis, “CIMS: a framework for infrastructure in- terdependency modeling and analysis,” in Proc. of the 2006 winter simulation conference, pp. 478–85; 2006.

[15] P. Zhang and S. Peeta, “A generalized modeling framework to analyze interdependencies among infrastructure systems,” in Transp Res Part B: Methodol, vol. 45, no.3, pp. 553–79, 2011.

[16] L. Svegrup, J. Johansson, and H. Hassel, “Integration of Critical Infrastructure and Societal Consequence Models: Impact on Swedish Power System Mitigation Decisions,” in Risk Analysis, in press. https://doi.org/10.1111/risa.13272

[17] A. Feoktistov, S. Gorsky, I. Sidorov, R. Kostromin, A. Edelev, and L. Massel, “Orlando Tools: Energy Research Application Development through Convergence of Grid and Cloud Computing,” in Communications in Computer and Information Science, vol. 965, pp. 289-300, 2019.

[18] A. Feoktistov, R. Kostromin, I. Sidorov, S. Gorsky, “Development of Distributed Subject-Oriented Applications for Cloud Computing through the Integration of Conceptual and Modular Programming,” in Proc. of the 41st International Convention on information and communication technology, electronics and microelectronics (MIPRO-2018), IEEE, pp. 256-261, 2018.

[19] A. Edelev and I. Sidorov, “Combinatorial Modeling Approach to Find Rational Ways of Energy Development with Regard to Energy Security Requirements,” in Lecture Notes in Computer Science, vol. 10187, pp. 317-324, 2016.

[20] A. Edelev, V. Zorkaltsev, S. Gorsky, V. B. Doan, and H. N. Nguyen, “The Combinatorial Modelling Approach to Study Sustainable Energy Development of Vietnam,” in Communications in Computer and Information Science, vol. 793, pp. 207-218, 2017.

[21] A. Feoktistov, I. Sidorov, A. Tchernykh, A. Edelev, V. Zorkalzev, S. Gorsky, R. Kostromin, I. Bychkov, A. Avetisyan, “Multi-Agent Approach for Dynamic Elasticity of Virtual Machines Provisioning in Heterogeneous Distributed Computing Environment,” in Proc. of the International Conference on High Performance Computing and Simulation, IEEE, pp. 909-916, 2018.

[22] A. Feoktistov, I. Sidorov, “Logical-Probabilistic Analysis of Distributed Computing Reliability,” in Proc. of the 39th International Convention on information and communication technology, electronics and microelectronics (MIPRO-2016), IEEE, pp. 247-252, 2016.

[23] J. Johansson, and H. Hassel, “An approach for modelling interdependent infrastructures in the context of vulnerability analysis,” in Reliability Engineering and System Safety, vol. 95, no. 12, pp. 1335-1344, 2010.

[24] Irkutsk Supercomputer Centre of SB RAS. [Online]. Available: http://hpc.icc.ru.