Information & Security: An International Journal

Brezhniev & Kharchenko, v.35, 2, 2016, 165-178 https://doi.org/10.11610/isij.3509

SMART GRID SAFETY AND SECURITY: EDUCATIONAL AND RESEARCH ACTIVITIES

Eugene BREZHNIEV and Vyacheslav KHARCHENKO

Abstract: Smart grid safety and security issues are of increasing interest to both researchers and practitioners. Universities invest considerable efforts in changing their curricula, developing new master and bachelor programs to respond to these new challenges. Currently, such courses and programs are not available in Ukraine. This paper presents our practical experience in developing such courses under Tempus projects. These programs might be based on the concept of research cases. The research case is an approach to research that focuses on gaining an in-depth understanding of a particular entity or event at a specific time. It includes the practical task settled by tutor, selection of methods by students, and presentation of results as a training paper. This approach might help to improve the student self-development, their knowledges and mental capabilities. It might facilitate their possible involvement into research activities focused on solving the problems of smart grid security and safety.

Keywords: research case, master program, cyber diversity, NPP, smart substation, common cause failures.

1 Introduction

Electricity industries are being transformed worldwide, driven by the need for more energy, urbanization, scarcity of natural resources and global warming. One of the most promising technologies is the smart grid technology which combines a traditional power grid with an "intelligent" information and communications technology (ICT) infrastructure to produce a smarter power system. The Smart Grid is an electrical power infrastructure that makes intelligent decisions about the state of the electrical power system to maintain a stable environment. The Smart Grid is an upgrade to the current electrical power system, so it has all of the functionality of our current power system plus several new functionalities.

Disturbances in smart grid 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, propagating into critical infrastructures such as Nuclear Industries, Telecommunication systems, transportation systems, etc.

The digital substations provide links between NPP and smart grid. Compared to other systems in an electric utility network, the smart substation has the highest density of valuable data needed to operate and manage a smart grid. The successful cyber-attacks on one of these substations could have fatal and expensive consequences, not only for all connected systems but for smart grid resilience and reliability.

It must be recognized that smart grid security and safety are interconnected issues and shall be treated simultaneously. They are evaluated by the similar methods and by people which have the common experience in traditional risk management. Both security and smart grid safety are important issues to be considered under the focus of educational and research activities performed by universities.

From practical point the smart grid cyber security and safety issues require well-trained proactive decision-taking operators of collaborating smart Grid stakeholders to operate the next generation smart grid infrastructure. To meet the increasing demand for ICT experts and ICT security experts with operational knowledge in electricity has become challenging and requires updating engineering and ICT education curricula.

Currently there are many attempts of EUs universities to address these challenging issues through development of the master and bachelor programs to accumulate knowledge and find the solutions in regard to this dynamic sector of power energy. For example, Grenoble Institute of Technology has developed the master in electrical engineering for Smart Grids and Buildings. It proposes a 20 month full time of state-of-art technical training in smart energy management in buildings and power grids together with economic, societal and cultural aspects to prepare students for solving smart grid related problems. Heriot Watt University organizes the master courses in Smart Grid Demand Management to progress students with an Electrical or Mechanical Engineering background to an expert in the understanding of a smart grid. These courses cover the resources (fossil and renewable), conversion technologies, electrical power generation, energy storage technologies, demand management, and energy economics.

The lack of master and bachelor courses devoted to smart grid reliability, safety and security shall be dealt with by many stakeholders, and one of them is university.

2 National Aerospace University's Efforts in Developing Master and Bachelor Courses Focused on Smart Grid Safety and Security

National Aerospace University KhAI (Kharkiv, Ukraine) has performed many projects focused on safety and security of ICT-based infrastructures. One is th TEMPUS SAFEGUARD project (National Safeware Engineering Network of Centres of Innovative Academia-Industry Handshaking, http://safeguard.csn.khai.edu/home) focused on breeding a new generation of engineering and research staff capable of performing constructive development in safeware engineering. One of results of this project is a development of master courses devoted to critical infrastructure safety assessment and assurance, development of the foundation of IT engineering of critical infrastructure. During this course the basic concept has been settled, the methods for safety of critical infrastructure were analysed and selected.

There is a second project focused on these issues. The aim of on-going TEMPUS GreenCo project (Green Computing and Communication, http://my-greenco.eu/) is to develop a master course focused on Research and Development of ITs for Smart Energy Infrastructures.

There are three modules. Module 1 is focused on mathematical Methods of Risk Assessment and Simulation of Smart Energy Infrastructures. Module 2 is focused on Fuzzy Methods and Information Technologies for Safety-Oriented Analysis of Smart Energy Infrastructures. Module 3 is devoted to development of Methods and Information Technologies for Security-oriented analysis of Smart Energy Infrastructures.

Module 1 has covered the following topics: 1. Introduction in smart energy infrastructure as a new green energy infrastructure, Overview of models and tools of SEI risk analysis. The practical activities for module 1 are supported by workshop devoted to benchmarking studies of smart grid risk analysis methodologies.

Module 2 includes the following topics: 1. Overview of SEI fuzzy safety analysis methods. 2. Overview of SEI tools for fuzzy safety analysis. The practical activities for module 2 are supported by practices focused on smart grid safety assessment with application of fuzzy logic toolbox. Module 3 includes the following topics: (1) Smart Energy Infrastructures security challenges; and (2) Overview of SEI tools for security analysis. The practical activities for module 3 are supported by practices focused on smart grid security assessment with application of Bayesian networks.

Smart grid security problems are addressed more deeply in other on-going smart grid related project, TEMPUS SEREIN (Modernization of Postgraduate Studies on Security and Resilience for Human and Industry Related Domains, http://serein.net.ua). This project has some modules devoted to Risk Analysis of SoS Security and Resilience, Smart grid security analysis and assurance. The main features of modules –

building and analysing the research cases settled to solve security tasks for digital I&C systems integrated under smart grid.

Basically the links between these projects could be depicted as shown on Figure 1.

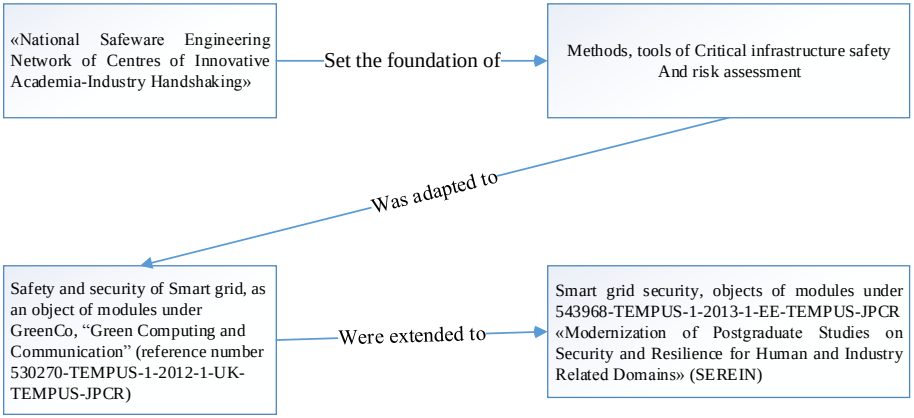

Figure 1: The relationships between smart grid issues addressed in SEREIN, GREENCO and SAFEGUARD projects.

The main features of modules that are to be developed during SEREIN project are research cases. The research case is an approach to research that focuses on gaining an in-depth understanding of a particular entity or event at a specific time. The researcher has to select the appropriate method and tools of investigation. It means that students have to analyse and select the appropriate set of methods. The results of such cases are arranged as a small scientific paper. This paper is not supposed to be published somewhere. The main aim of such activities is to train the students to prepare the scientific papers. The main components of research case are the following:

- Practical tasks;
- Methods;
- Training papers.

The relationships between stages of a research task are given on Figure 2.

Figure 2: The relationships between stages of a research task.

The main objective of this paper is to describe the research case to be used during practical task. This research task is focused on cyber diversity assessment of smart grid substation with critical load.

3 Description of Research Task's Stages

3.1 Obtain a Research Task

Nowadays there are no differences among smart grid substations in respect to cyber security. Smart substations main assets are not only physical facilities, but also information, databases and software applications, different intelligent electronic devices (IEDs) such as breaker controllers, voltage regulators, remote terminal units (RTUs), programmable logic controllers (PLCs). These IEDs are important cyber assets of digital substation.

Industrial Control Systems (ICS) have common cyber vulnerabilities.[1] These vulnerabilities are divided in three general categories: the vulnerabilities inherent in the ICS product, vulnerabilities caused during the installation, configuration, and maintenance of the ICS and the lack of adequate protection because of poor network design or configuration. For example, through bad coding practices and improper input validation, access can be granted to an attacker allowing them to have unintended functionality or privilege escalation on the systems. Examples of improper input validation identified are within buffer overflows, boundary checking, and code injection. It means that besides hardware CCFs digital substations' IEDs might be prone to cyber common cause failures (CCCFs). Cyber CCFs might be determined as events when cyber assets' availability, confidentiality and integrity are compromised within a specified (short) time interval. The reasons are the common vulnerabilities, tough coupling within networks between IEDs which might lead to security violation due to human errors, shared input data equipment, environmental events (flooding, storm) and cyber attacks. Thus substations with critical loads, such as NPPs, should be given the highest level of importance in respect of their cyber security. The higher level of cyber security of smart substation with critical load might be achieved through implementation of substations' variety when IEDs with similar functionalities are different and less vulnerable to the same shared cause.

A study by the Homeland Security's National Cyber Security Division The document analysed common vulnerabilities of a large variety of systems, and provided tailored assessment and methodology aimed to deliver most value to the customer.[2] In this analysis, all vulnerability identification activities were focused on enabling the identification and remediation of the highest risk ICS cybersecurity vulnerabilities rather than the collection of data for statistical purposes. It also provides recommendations for ICS vendors and owners on how to reduce the common vulnerabilities of ICS systems. The list of recommendations includes the following: create a Security Cul-

ture; Enhance ICS Test Suites; Create and Test Patches; Redesign Network Protocols for Security, etc. It might be unfeasible to implement the joint plan for common vulnerabilities reduction considering such business issues as competition among vendors, lack of coordination, etc.

A report by the power management solutions' provider Eaton considers the application of "defence in depth" for cyber security assurance of electrical distribution systems.[3] "Defence in depth" is a strategy of integrating technology, people, and operations capabilities to establish variable barriers across multiple layers of an organization. These barriers include electronic countermeasures such as firewalls, intrusion detection software/components, and antivirus software, coupled with physical protection policies and training. The cost of implementation of such strategy is not considered in this paper.

Sandia National Laboratories in Albuquerque, New Mexico, also considered common vulnerabilities of control systems.[4] Their report describes the generalized trends in vulnerabilities observed from the assessments, as well as typical reasons for these security issues and the introduction to an effective mitigation strategy. Many of these vulnerabilities result from deficient or non-existent security governance and administration, as well as budgetary pressure and employee attrition in system automation. It is also mentioned that defence-in-depth concept should be used to cyber security assurance of cyber components.

It might be noted that the application of smart grid substation variety (diversity) is not considered as a means to decrease CCFs of IEDs including cyber CCFs. There is also no analysis of impact of substation diversity on probability of event when these substations with critical load are failed due to one shared cause. This event is determined as substations CCFs when all of them got unavailable within one short time interval.

Diversity is one of the general principles used to decrease hardware vulnerability against CCF and provide dependability of I&C. Differences in equipment, development and verification technologies, implemented functions, etc. can mitigate the potential for common faults.

Generally, the logical structure of the smart substation includes: the process level where the digital signal acquisition, consolidation, processing operations are performed; interval layer measurement and control; station control layer that achieves communication within substation and control system as well as coordination with the substation operational function and the station-level support function based on information sharing. Many of these functions are performed by IEDs.

Due to high level of coupling and interconnections between IEDs they might be prone to hardware and software failures.

All of these events put the new risks to smart grid safety, reliability and security. The practical task that is settled to student is to evaluate the difference between IEDs to minimize the risks of hardware and software failures.

The approach for solving this task is given below. The approach deals with qualitative aspects represented in qualitative terms by means of linguistic variables. Computing with words (CW) has been applied as a computational basis to linguistic decision making of complex situations.[5]

To select the most diverse smart grid substations, using the diversity criteria and evaluate the similarity (difference) between IEDs, expert should take into consideration the compelling evidence. Based on these evidences experts evaluate the difference (similarity) between similar IEDs (from different substations) using the linguistic terms: SAME (S), NEARLY SAME (NS), DIFFERENT (D).

The following diversity strategies of IEDs smart substations implementation are considered in this paper:

- Strategy S_{11} – All smart substations and their IEDs are similar. One vendor develops and produce all substations with no difference in IEDs design, manufacturing, cyber issues, etc.;
- S_{21} – All substations are different and produced by different vendors;
- S_{31} – All substations' IEDs are produced by one vendor but there are some differences between them.

During this stage experts are supposed to fill the comparison matrixes to evaluate the similarities (differences) between the IEDs in term of hardware and cyber aspects. The expert is supposed to compare the IEDs with similar functionalities from different substations and select the most different between them.

If the particular IED for the first substation is determined then it is required to compare it with the possible alternatives for IEDs with similar functionalities from second and third substation. If the substation automation controller, for example, OM600, the grid automation controller of ABB, is selected for the first substation, according to S2 strategy, this IED is compared with C264 from Alstom Grid (IED1), GE's D25 from General Electric (IED2) and SICAM (IED3) AK from Siemens. The expert is required to assign the weight of each criterion. The criterion's weight might be expressed either as linguistic value (Low, Medium, High) or any numerical values from [0, 1]. For sake of simplicity the weight of criterion is presented as a scalar value. Table 1 represents the example of diversity assessment for the strategy S_{21} (hardware aspects).

Table 1: Check List for IEDs CCF (Hardware Vulnerabilities Aspect).

Vulnerabilities criterion	W_k, weight of criterion	IEDs		
		IED1	*IED2*	*IED3*
Design				
System Layout/Configuration	0,2	NS	D	NS
Component Internal Parts	0,23	NS	D	D
Design team	0,13	D	D	D
Design procedures	0,24	NS	D	NS
V&V procedures	0,2	NS	D	NS
Manufacturing				
Manufacturing method, and material	0,13	NS	NS	NS
The manufacturing staff	0,27	D	D	D
The same quality control procedure	0,6	NS	NS	NS
Installation				
Installation method, and material	0,33	NS	NS	NS
The Installation staff	0,41	D	D	D
The quality control procedure	0,26	D	D	NS
Operation				
Operation method, and material	0,4	S	NS	S
The Operation staff	0,32	D	D	D
The quality control procedure	0,28	NS	NS	D
Maintenance				
Maintenance/ Test/Calibration Schedule	0,21	NS	D	NS
Maintenance/ Test/Calibration Procedure	0,31	NS	D	NS
Maintenance/Test/Calibration Staff	0,48	D	D	D

Table 2 presents the example of diversity assessment for the set of strategies S_{21} (cyber aspect).

Table 2: Check List for IEDs CCF (Cyber Vulnerabilities Aspect).

Vulnerabilities criterion	W_k, weight of criterion	IEDs		
		IED1	*IED2*	*IED3*
Design				
The coding practices	0,12	NS	D	D
The security requirements	0,21	NS	D	D
The security testing procedure	0,13	NS	NS	NS
The vendor	0,15	D	D	D
The tools used	0,19	S	S	NS
The security culture	0,2	NS	S	D
Installation				
The installation procedure	0,43	D	D	D
The installation team	0,35	D	D	D
The installation tool	0,22	NS	NS	NS
Operation				
The communication links	0,51	S	NS	NS
The port security on network equipment	0,49	NS	D	NS
Configuration				
Patch management procedure	0,22	NS	NS	D
Encryption procedure	0,13	D	NS	NS
Authentication procedure	0,65	D	D	D

The expert is proposed to use linguistic values to evaluate all possible IEDs' alternatives for substations. In this paper, we shall use labels represented by triangular fuzzy numbers. A triangular fuzzy number, denoted by M = <m, α, β>, has the membership function:

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

The point m, with membership grade 1, is called the mean value and α, β are the left hand and right hand spread of M respectively. For example, we assign the following semantics to the set of three terms:

NS = (0, 0,25, 0,5), S = (0,25, 0,5, 0,75), D = (0.5, 0,75, 1).

During the aggregation stage all linguistic values provided by experts are aggregated to obtain a collective assessment for the IED's alternatives. It is provided by calculation of the fuzzy diversity score D_{ij} as an arithmetic mean:

$$D_{ij} = (\frac{1}{t}\sum_{i=1}^{t} w_k \times m_{ij}^t, \frac{1}{t}\sum_{i=1}^{t} w_k \times \alpha_{ij}^t, \frac{1}{t}\sum_{i=1}^{t} w_k \times \beta_{ij}^t) \quad (2)$$

where w_k – weight of *k* criterion; $<m_{ij}^t, \alpha_{ij}^t, \beta_{ij}^t>$ – a triangular fuzzy number that represents one of linguistic values {S, NS, D} assigned by t^{th} expert for S_{ij} diversity strategy. D_{ij} represents a difference between two IEDs. The more value D_{ij}, which corresponds certain diversity strategy S_{ij}, the more diverse both IEDs.

Using the best-fit method,[5] the obtained fuzzy diversity score D_{ij} for each IEDs can be mapped back to one (or all) of the defined linguistic terms (SAME, NEARLY SAME, DIFFERENT). The method uses the distance between fuzzy diversity score, represented by fuzzy triangular number for each IEDs and each of the initial linguistic terms to represent the degree to which obtained score, is confirmed to each of them. The distance between the obtained fuzzy diversity score D_{ij} and the expression SAME, NEARLY SAME, DIFFERENT is defined as follows:

$$d_{ij}^{(r)}\left(D_{ij}, SAME\right) = \left[\sum_{j=1}^{3}(\mu_{Dij}^j - \mu_{same}^j)^2\right]^{\frac{1}{2}}$$

$$d_{ij}^{(r)}\left(D_{ij}, NEARLY\ SAME\right) = \left[\sum_{j=1}^{3}(\mu_{Dij}^j - \mu_{NS}^j)^2\right]^{\frac{1}{2}} \quad (3)$$

$$d_{ij}^{(r)}\left(D_{ij}, DIFFERENT\right) = \left[\sum_{j=1}^{3}(\mu_{Dij}^j - \mu_{different}^j)^2\right]^{\frac{1}{2}}$$

Hence, each IED is characterized by 3-tuple $<d_{ij}^{(1)}, d_{ij}^{(2)}, d_{ij}^{(3)}>$, where , $d_{ij}^{(r)}$ is the distance between obtained fuzzy diversity score and corresponding linguistic term (SAME, NEARLY SAME, DIFFERENT).

It should be noted that each , $d_{ij}^{(r)}$ (j = 1,…J, where j – number of possible alternatives classified as type of S_i strategy) is an unsealed distance. The closer D_{ij}, is to the r^{th} expression, the smaller $d_{ij}^{(r)}$ is. More specifically, $d_{ij}^{(r)}$ is equal to zero if D_{ij}, is just the same as the r^{th} expression in terms of the membership functions. In such a case, D_{ij} should not be evaluated to other expressions at all due to the exclusiveness of these expressions. To embody such features, new indices need to be defined based on $d_{ij}^{(r)}$ (r = 1, 2, 3).

Suppose $d_{ij}^{(3)}$ is the smallest among the obtained distances for D_{ij}, and let α_{i1}, α_{i2}, α_{i3} represent the reciprocals of the relative distances between the identified fuzzy diversity score D_{ij}, and each of the defined linguistic terms with reference to $d_{ij}^{(3)}$(smallest distance). Then, $\alpha_{ij}^{(r)}$ (r= 1, 2, 3) can be defined as follow:

$$\alpha_{ij}^{(r)} = \frac{1}{\frac{d_{ij}^{(r)}}{d_{ij}^{(3)}}}, \; r = 1,2,3. \tag{4}$$

If $d_{ij}^{(3)}$ = 0 it follows that $\alpha_{ij}^{(3)}$ is equal to 1 and the others are equal to 0. Then, $\alpha_{ij}^{(r)}$ (r = 1, 2, 3) can be normalized by:

$$\beta_{ij}^{(r)} = \frac{\alpha_{ij}^{(r)}}{\sum_{r=1}^{3} \alpha_{ij}^{(r)}}, \; r = 1,2,3 \tag{5}$$

Each $\beta_{ij}^{(r)}$ represents the extent to which D_{ij} belongs to the r^{th} defined linguistic terms. Thus, $\beta_{ij}^{(r)}$ could be viewed as a degree of confidence that obtained fuzzy scores for all diversity strategies S_{ij} belong to the r^{th} defined linguistic terms.

Results obtained for the selection of the most diverse substation controller to decrease the cyber vulnerability of smart substation with critical load are presented in the table 3. The IED1 is the most diverse IED to OM600 in respect to cyber vulnerabilities.

Next, all IEDs' alternatives are ranked by using the collective linguistic assessment obtained in the previous stage, taking into account the cost of each IED, Cij. The rational diverse strategy could be found with the following criterion:

Table 3: Results Obtained for All IEDs Considered in Example.

IED alternatives	Degree to which D_{ij} belongs to the initial terms		
	S	NS	D
IED1	0,12	0,39	0,49
IED2	0,36	0,28	0,38
IED3	0,33	0,63	0,04

$$S_{ij}^{*} = argmax \frac{\beta_{ij}^{(r)}}{C_{ij}^{*}} \quad (6)$$

where $\beta_{ij}^{(r)}$ represents the extent to which D_{ij} belongs to the r^{th} defined linguistic terms; C_{ij}^{*} - cost of S_{ij} reduced to $\sum C_{ij}$, ij – number of alternatives.

The main aim of all stages described above is decrease the IDEs cyber common vulnerabilities of substations with critical load.

3.2 Select a Method (Tool)

The approach given above is focused on evaluation of difference between IEDs based on set of given criteria. This stage is the most challenging stage of research case. Her students have to analyse the most appropriate methods which might be used to the same purpose – assess the difference between IEDs. If student cannot generate any ideas he (she) might use the approach given above with a small variation in task. The students are supposed to suggest the new approach to evaluate IEDs difference. The set of criteria might be left unchanged.

3.3 Training Paper

This stage is very important for students' research progress. During this stage each student is supposed to write a training scientific paper which presents the results obtained during previous stages. The requirements to this paper are explained during a training session. The students might work together to present a joint paper. The time for paper preparation is limited.

4 Conclusions

The challenges to safety and security of smart grid have to be considered under the focus of educational and research activities at universities. This might be taken into account when the corresponding master and bachelor programs are developed. The set of research cases will be developed to support the modules focused on Safety and security analysis of ITS (Intellectual Transportation Systems), Smart grid security analysis, Smart grid security assurance. The following list of topics are to be included into the smart grid security analysis and assurance modules (for both 60 hours): regulatory security requirements for critical ICS (in nuclear domain as well), ICS challenges and security concerns methods and tools for ICS security assessment, ICS vulnerabilities, methods for prognosis of attack vectors in ICS. The list of topics will include the issues related to ICS secure development, including software and hardware aspects, recommendations and countermeasures, ICS Security Controls etc.

The module (time – about 30 hours) focused on vehicle cyber security (ITS security) will be supported by research cases. These research cases will be done for the following topics: Cyber Security Threats for ITS, methods for ITS security risk assessment, development of approaches for ITS security risk assurance, etc.

This approach allows hitting the following targets: to educate future operators of smart grid and breed new generation of researches in this area. Smart grid master and bachelor programs might be based on the concept of research cases. This approach might help to improve the student self-development, their knowledge and mental capabilities. It might stipulate their possible involvement into research activities focused on solving the smart grid security and safety problems.

Acknowledgment

This article reflects results within the SEREIN project (Project Reference: 543968-TEMPUS-1-2013-1-EE-TEMPUS-JPCR) that has received funding from the European Community's TEMPUS IV programme under the Sixth Call for Proposals EACEA/35/20112.

References

1. *NSTB Assessments Summary Report: Common Industrial Control System Cyber Security Weaknesses*, Report INL/EXT-10-18381 (Idaho Falls, ID: Idaho National Laboratory, 2010). Accessed April 19, 2016. https://fas.org/sgp/eprint/nstb.pdf.
2. Common Cybersecurity Vulnerabilities in Industrial Control Systems (Washington, D.C.: Homeland Security, Control Systems Security Program, National Cyber Security Division, May 2011). Accessed April 27, 2016. https://ics-cert.us-cert.gov/sites/default/files/recommended_practices/DHS_Common_Cybersecurity_Vulnerabilities_ICS_2010.pdf.

3. Max Wandera, Brent Jonasson, Jacques Benoit, et al., *Cybersecurity Considerations for Electrical Distribution Systems*. White Paper WP152002EN (Cleveland, OH: Eaton, March 2014). Accessed May 26, 2016. www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf.
4. Jason Stamp, John Dillinger, William Young, and Jennifer DePoy, *Common Vulnerabilities in Critical Infrastructure Control Systems*, 2nd edition (Albuquerque, NM: Sandia National Laboratories, 2003). Accessed May 28, 2016. http://energy.sandia.gov/wp-content/gallery/uploads/031172C.pdf.
5. Lotfi A. Zadeh and Janusz Kacprzyk, eds., *Computing with Words in Information/ Intelligent Systems – Part 1: Foundations* (Berlin Heidelberg: Springer, 1999).

About the Authors

Dr. Eugene BREZHNIEV and Prof. Vyacheslav KHARCHENKO are with the National Aerospace University KhAI, Kharkiv, Ukraine.