Challenges and necessities of vulnerability assessment for electricity infrastructures

CHALLENGES AND NECESSITIES OF VULNERABILITY ASSESSMENT FOR POWER SYSTEMS INFRASTRUCTURES

Senior Ass. Researcher **Tao HUANG,** PhD[1], Eng. **Simona Louise VORONCA[2],**
Professor **Anca Alexandra PURCAREA** PhD[3], Eng. **Abouzar ESTEBSARI**[1]

[1]Polytecnic university of Turin, Department of Energy, Turin, Italy
[2] CN Transelectrica SA, Romania
[3]University Politehnica of Bucharest, Faculty of Entrepreneurship, Business Engineering and Management, Romania

REZUMAT. O serie de studii şi definiţii ale vulnerabilitatii sistemelor electro-energetice au fost publicate, cu luarea în consideraţie a multiplelor aspecte complexe, dar conducând la ambiguităţi în utilizarea practică. De aceea, în această lucrare se propune o clasificare clară pentru evaluarea vulnerabilităţii, cu izolarea diferitelor origini. Prin aceasta structurare se pot evidenţia si prioritiza ameninţările, obţinându-se o mai buna înţelegere a punctelor slabe in care se pot dezvolta vulnerabilităţi. Un model generic pentru vulnerabilităţile sistemului electro-energetic, în special al celor operaţionale, poate fi dezvoltat ulterior, in vederea diminuării acestora.

Cuvinte cheie: lanţ de evenimente, sistem electro-energetic, securitate, susceptibilitate, vulnerabilitate

ABSTRACT. Many studies and definitions of vulnerability have been published considering multiple aspects collectively which resulted in ambiguities in practical use. Therefore, a clear classification for vulnerability assessment isolating different dimensions of the origins of vulnerability is proposed in this paper. Under the framework, focuses can be brought on a specific dimension for a better understanding of where the system vulnerability arises. A generic pattern of system vulnerabilities, especially operational vulnerabilities, can be subsequently developed for its mitigation.

Keywords: Chain of events, Power systems, Susceptibility, Security, Vulnerability

1. INTRODUCTION

With entanglement of the power systems infrastructures with other critical fundamental infrastructures rather than traditionally vertical and self-sustained system, as well as the internal changes inside the power system, such as growing penetration of renewable energy sources, deepening markets and development of the ICT systems, electricity infrastructures are more vulnerable to the threats that could happen to any aspect of the "open" system nowadays.

The rapid and massive deployment of renewable energies based distributed generation and "intelligent" equipment provides much more potentials for the system to fail. For example, the introducing of smart meters provides a large number of access points to hackers to initiate malicious cyber attacks; the shift of pure consumers at the final end to prosumers with distributed generation using renewable energies such as photovoltaic panels and micro-CHPs alters the easily controllable unilateral power flow to ad hoc bilateral power flows. These changes generate new vulnerable points in the systems that have never been foreseen. Therefore, the necessities of vulnerability analysis system for electricity infrastructures are urgently needed to be addressed.

Although vulnerability draws many attentions, there is no common definition widely accepted. Thywissen [1] lists 29 different definitions for the term vulnerability in the literature due to different purposes of the studies. Most of the definitions are related to vulnerability of societies but not the vulnerability of the system itself. Similarly, differences of definitions of vulnerability can be found for different infrastructures as well [2 – 8]. Despite of the verities in the definitions, a common characteristic of vulnerability is implied that system vulnerability is closely connected to the system ability to keep its functionality when exposed to materialized threats. In some definitions, the ability of function restoration is also included [1]. In addition, several factors (physical, social, economic, and environmental) that have an influence on the vulnerability of a system can be considered [3 – 7].

To identify the vulnerability, two aspects must be involved: threat capability and control strength [17]. Threat capability is a measure of the severity of a possible incident in terms of the gravity of the damage it may cause, while a control refers to the measures or changes which reduce its vulnerability. For example, a transmission line might be destroyed by a storm, which depends on the severity of the storm itself and the

strength of the line forged by the length and construction materials. Although the example demonstrates the two key aspects of the vulnerability consideration, it only concerns a component of the system. In contrast, vulnerability of a system is more complex and inclined to evaluate the operative functionalities of the system with multiple components dynamically respond to the changes triggered by a threat. Therefore, vulnerability identification of the system may refer either to the system susceptibility (tendency of the system creating unwanted events subject to a threat), or to an explicitly designed countermeasure against a certain threat.

Most of the current vulnerability studies differentiate component vulnerability and system vulnerability, which makes the terminology and results ambiguous and impractical to use. Moreover, besides the component or the system points of view, vulnerability can also be observed from structural and operational dimensions. Therefore, we firstly need to clarify the vulnerability evaluation system by providing a framework which isolates different considerations and views in vulnerability studies. In this way, we can describe the origins of the vulnerability distinctively.

2. CALSSIFICATION OF VULNERABILITY ASSESSMENT FOR ELECTRICITY INFRASTRUCTURES

Various frameworks for vulnerability evaluation have been proposed in previous studies with specific focuses, such as individual components, effects, etc. For example, reference [9], proposed a method for assessing voltage security and ranked vulnerable buses with respect to voltage security only. Therefore, the results of such studies would be difficult to be applied to a broader and generic scenario. However, one of the purposes of a vulnerability analysis is to identify events during the evolutions of the failure (a chain of events) leading to critical situations with huge negative consequences.

In this paper, we propose a framework to isolate different aspects so that we can concentrate on each specific origin of vulnerability, which could eventually facilitate the development of system responses to possible crisis situations and create an awareness of vulnerability management and the necessity of such assessments.

Two general aspects of vulnerability evaluation would be studied either from the structural point of view or from the operational point of view. So, the evaluation system should be divided into two the aspects firstly as shown in figure 1.

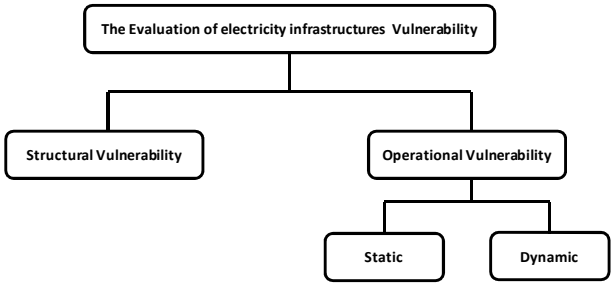

Fig. 1. Classification of vulnerability assessment for electricity infrastructures

Structural Vulnerability. Structural vulnerability refers to the weakest components or their interconnections in the topologies of the physical infrastructures which could cause a large loss of system functionalities. Morakis et al. [10] define vulnerability as a "measure of the exploitability of a weakness". In structural engineering, the term vulnerability is often used to capture the "susceptibility of a component or a system to some external action". Thus, a structure is vulnerable if "any small damage produces disproportionately large consequences" [11].

Structural vulnerability intrinsically depends on the structure of the network and is independent from the operational status of the system. Power system structural vulnerability is based on the graphical representation of a network considering the specificities of power systems; therefore it is a physical property of the system, which means even if the system is not in operation, the structural vulnerable points still exist. However, in order to observe this kind of vulnerabilities, operation is needed to exceed the maximal capability of these vulnerable points.

Many researchers have embraced the idea of structural vulnerability and made pioneer studies on the power systems. For example, an analysis of the structural vulnerability of the Italian power grid, using a graph-based model of cascading failures can be found in [12]. Carreras et al. [13] use a linear approximation and standard optimization to represent cascading transmission line overloads to identify the vulnerable branches in the system.

Operational Vulnerability. Operational vulnerability refers to the most dangerous phenomena that can lead to a large loss of system functionalities during the operation. Large loss of system functionalities is usually caused by cascading failures leading to operational constraints violations (usually static problems like overload, over voltage, etc.) or instabilities (usually dynamic problems, like oscillation, loss of synchronization, etc.) in the power grids. Power system instability can be caused by transient instability, dynamic instability or voltage instability [18]. Therefore, not only the static aspect is interesting to be

studied for the operational vulnerability, but also dynamic phenomenon should be included.

The system operation status is constantly changing; therefore, the operational vulnerability is shifting accordingly and not easy to detect and define. One of the most challenging problems is that system operators have no precise idea of the system security. During the operation, they may face insecure states due to events much different from what were predicted in the planning and other online/off-line studies. Since such events are somehow unexpected, the operators do not have enough security information or available resources/countermeasures to take timely preventive or emergency control actions. There were several large blackouts illustrating it: In July 1987 the system operators of TEPCO (Tokyo Electric Power Company) just watched their system voltage decreasing while the load was increasing fast till voltage collapse occurred after they run off their reactive power supply[14]; In August 1996, the BPA operators did not know that their system was insecure after a key transmission line was disconnected following several line outages in the Western Interconnection System[15] [16]; in July 1996, a large area blackout happened in Idaho, which the system simulations after that showed that if appropriate load shedding had been taken at that area for half an hour, the blackout could have been prevented [15,16].

It is manifest that the blackouts listed in the above examples are closely related with the operational vulnerabilities. The cascades might have been limited to a certain extend if the operational vulnerabilities can be detected ex ante with more general approaches and tools. To quickly scan the operational vulnerability under emergencies usually requires a lot of calculations with multiple focuses on different aspects and events. If there is a generic pattern pointing out where the system operation would most probably go wrong, attentions can be focused primarily on the most vulnerable points in the operation.

Nevertheless, it is not easy to form the common pattern purely by simulation. The observation from history of blackouts and the corresponding chains of events can be efficiently provides information to identify the most operational vulnerability of a system. For forming the common paten, firstly the most vulnerable elements of the network after the materialization of a threat need to be identified, and then the most probable effects of failures of such vulnerable components need to be captured. This also requires the study of the evolution of the system in operation during the cascades, which enhance the operational vulnerability.

In this way, studies of the historic blackouts are needed as an efficient way of vulnerability observation.

3. CONCLUSIONS

Vulnerability assessment has been always a challenging concern in power systems, and there have been many studies conducted to evaluate different aspects of vulnerabilities. However, there is no general classification framework which clearly individualizes each aspect of vulnerabilities from components to system, and from structural point of view to the operation level. From the system vulnerability point of view, we discussed that the vulnerability could emerge not only from the structure but also from the operation. Therefore, we proposed a framework to isolate different aspects to enable the detection of the origins of the system vulnerable points. Considering the difficulties of detecting operational vulnerability, studying of the cascading failures (chain of events) in historic blackouts could provide an excellent observation as to from where the vulnerability arises in operation.

Under this framework, deliberately designed tool to quickly grasp a specific blackout without too many details can be employed to abstract the common pattern of operational vulnerabilities. In this way, the analysis could help to improve the system incident response to possible critical situations and provide a basis for prioritizing among different possible vulnerable points.

ACKNOWLEDGMENTS

This paper has been produced with the financial assistance of the SESAME project (a FP7-security project supported by the European Commission, aiming at providing a contribution to the development of tools and a regulation framework for the security of the European power grid against natural, accidental and malicious attacks. https://www.sesame-project.eu/). The views expressed herein are those of the authors and can therefore in no way be taken to reflect the official position of the European Commission.

BIBLIOGRAPHY

[1] **Thywissen, K**.: *Core terminology of disaster reduction*. In: Birkmann,J., editor. Measuring vulnerability to natural hazards: Towards disaster resilient societies, United Nations University Press, Hong Kong 2006.

[2] **NOU. Når sikkerheten er viktigst:** *Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner*. NOU 2006:6, Oslo 2006.(In Norwegian)

[3] **Holmgren, Å. J.:** *Quantitative Vulnerability Analysis of Electric Power Networks.* Doctoral Thesis. Royal institute of Technology, Stockholm 2006.

[4] *DEMA. DEMA's Approach to Risk and Vulnerability Analysis for Civil Contingency Planning*. Internet document. Background_paper_on_DEMAs_approach_to_risk_and_vulnerability, Accessed 2011-04-08.

[5] Commission of the European Communities. *Green paper on a European programme for critical infrastructure protection*. Commission of the European Communities, Brussel 2005.
[6] President's Commission on Critical Infrastructure Protection. Critical foundations - *Protecting America's infrastructures*. The Report of the President's Commission on Critical Infrastructure Protection, 1997.
[7] *United Nations International Strategy for Disaster reduction (UN/ISDR): Living with Risk: A global review of disaster reduction initiatives.* United Nations publications, Geneva 2004.
[8] **Kröger, W., Zio, E**.: *Vulnerable Systems*. Springer, London 2011
[9] **Amjady, N. & Esmaili**, M. (2003) "*Improving voltage security assessment and ranking vulnerability buses with consideration of power system limits*". Electrical Power and Energy Systems 25, pp. 705—715.
[10] **Morakis, E., Stylianos, V. & Blyth, A.** (2003). "*Measuring vulnerabilities and their exploitation cycle*". Information Security Technical Report 8, pp. 45-55.
[11] **Agarwal, J., Blockley, D. & Woodman, N.** (2003) "*Vulnerability of structural systems*". Structural Safety 25, pp. 263—286.
[12] **Crucitti, P., Latora, V. & Marchiori, M.** (2004) "*A topological analysis of the Italian electric power grid*" Physica A 338, pp. 92-97.
[13] **Carreras, B. A., Lynch, V. E., Dobson, I. & Newman, D. E.** (2004) "*Complex dynamics of blackouts in power transmission systems*". Chaos 14, pp. 643-652.
[14] **A. Kurita, T. Sakurai,** "*The power system failure on July 23, 1987 in Tokyo*", in 1988 Proc. Of the 27th Conference on Decision and Control, Dec. 1988, pp. 2093 –2097.
[15] **C.W. Taylor,** "*Improving grid behavior*", IEEE Spectrum, vol. 36 (6), pp. 40-45, June 1999.
[16] NERC Disturbance Analysis Working Group, "*Western Interconnection (WSCC) System Disturbance* — August 10, 1996", NERC 1996 System Disturbances Report, Aug 2002, Available: http:// www.nerc.com
[17] SESAME, "*VULNERABILITY AND THREAT KNOWLEDGE BASE*",Deliverable D1.2 of the FP7 EU project on Securing the European Electricity Supply Against Malicious and accidental threats, September 2011.
[18] **H.F. Latorre , M. Ghandhari ,** "*Improvement of power system stability by using a VSC-HVdc*", International Journal of Electrical Power & Energy Systems, Volume 33, Issue 2, February 2011, Pages 332–339

About the authors

Senior Ass. Researcher. **Tao HUANG,** PhD
Polytechnic University of Turin, Department of Energy, Corso Duca degli Abruzzi, 24, 10129 Torino , Italy.
email:tao.huang@polito.it

Senior Assistant Researcher at department of energy of polytechnic university of Turin (POLITO), graduated from department of electrical engineering of POLITO. Since 2010 he has been working as WP leader, Executive Vice Coordinator on a FP7 project SESAME (Securing the European Electricity Supply Against Malicious and accidental thrEats) cofunded by the European Commission. https://www.sesame-project.eu/) supported by the European Commission. His research interests are: energy systems security, complex systems theories and applications in networked systems vulnerability identification and electricity markets, interoperability of multi-layer systems, etc.

Eng. **Simona Louise VORONCA**, MSc, PhD Student
CN Transelectrica SA, Romania, Integrate management Department, Risk Management, Olteni 2-4 street, Bucharest
email: simona.voronca@transelectrica.ro

In charge with Risk management, in the Romanian Transport and System Operator, graduated from University Politehnica of Bucharest, Power Faculty and Academy of Economic Studies Bucharest, MSc in Risk Management. In the energy industry throughout all career, with experience in the areas of risk management & business continuity planning, is among the pioneers in Risk management practices in Romania. She has been involved in multinational collaborative research as expert and evaluator for the FP7 European Commission Projects.

Professor **Anca Alexandra PURCAREA,** PhD
Dean of Faculty of Entrepreneurship, Business Engineering and Management, University Politehnica of Bucharest, str. Splaiul Independentei 313, Sector 6, Bucharest, Romania
email: apurcarea@gmail.com

Supervisor at the Doctoral School of Entrepreneurship, Business Engineering and Management, with a advanced expertise in the development of complex models for the optimization of solutions aiming the national economy sustainable development, senior researcher in the fields of company management and environmental protection, with contribution in more than 50 scientific research contracts. She is evaluator within various national research programmes i.e. RELANSIN, CEEX and CNCSIS. She has published 16 technical books and more than 80 articles and scientific papers.

Eng. **Abouzar ESTEBSARI**, PhD Student
Polytechnic University of Turin, Department of Energy, Corso Duca degli Abruzzi, 24, 10129 Torino , Italy.
email:abouzar.estebsari@polito.it

A doctoral researcher at the Polytechnic University of Turin in the department of energy, graduated at Shahed University of Tehran with a master degree in electrical engineering in 2009 and graduated as a bachelor of electrical engineering at Iran University of Science and Technology in 2006. Since March 2012 he has been working on a FP7 (Securing the European Electricity Supply Against Malicious and accidental thrEats) cofunded by the European Commission.