A FRAMEWORK FOR RANKING THREATS AGAINST POWER SYSTEMS SECURITY

Senior Ass. Researcher **Tao HUANG,** PhD[1], Eng. **Simona Louise VORONCA[2],**
Professor **Anca Alexandra PURCAREA** PhD[3], **Ying Jun WU,** PhD [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. Analizand diferitele ameninţări posibile şi modul în care acestea afectează sistemele energetice, lucrarea se concentrează asupra studiului preliminar de dezvoltare a unui model - cadru pentru o evaluare calitativă şi cantitativă a ameninţărilor. Este prezentat chestionarul conceput pentru a capta opiniile experţilor , ca prim pas pentru evaluarea ameninţărilor majore posibile la adresa securităţii sistemelor energetice, din perspectiva operatorilor de sisteme de transport al energiei electrice din Uniunea Europeana. Evaluările primite de la experţi reprezintă date de intrare si vor fi prelucrate prin metoda Procesul reţelei analitice.

Cuvinte cheie: procesul reţelei analitice, sistem energetic, prioritatea ameninţărilor, securitate

ABSTRACT. Based on different possible threats and of the way they affect power systems, this paper focuses on the preliminary trial to develop a framework for a qualitative and quantitative threats assessment. It is aimed to present the questionnaire designed to capture experts' opinions as the first step proposed to evaluate the major possible threats against power system security and a rank of threats in EU from the Transmission System Operators' perspective. Analytic network process was employed for processing the received evaluations from experts.

Keywords: analytical network method, power systems, threats ranking, security

1. INTRODUCTION

Due to the large exposure to the outside environment such as wide geographic expansion, unprotected equipment in the fields, excessively relying on digital communication systems, etc., the power system is vulnerable to many potential threats. Generally, threats against the security of power system operation can be classified into the following categories (Table 1) [1, 2]:

Table 1. Threats Classification

CAT.	NAT.	THREAT	DEFINITION
Conventional	Non-intentional	Natural threats	*Natural events not strictly controlled by human that if happen may impact the power system operation causing damages* (geomagnetic storms, earthquakes, forest fires, tsunamis, hurricane, flood, lightening, hail, animal, etc.).
		Accidental threats	*Possible failure of network devices and the wrong human decisions that may threat power system operation* (operational fault, system equipment failure, accident due to the poor management, etc.).
Emerging	Intentional	Malicious threats	*Possibility of intentional actions against power systems facilities and operation, which are undertaken by different agents* (terrorist, criminal group, cyber attackers, copper theft, vandal, psychotic, malware writer, etc.) by various means (explosives, high power rifles, malware, etc.) with the willingness to cause damage for getting political or economical benefits.
	Non-intent.	Systemic threats	Potential failures brought by the evolution of power systems and new technologies (high penetration of renewable energies, bidirectional power flows from prosumers, etc.)

Threats from different catalogues have totally different features. For example, the natural threats happens unintentionally with huge impacts on a large area and humanly impossible to prevent their happening; while malicious threats happens with great intention and human efforts can strategically prevent it from happening or diminish their consequences. In

addition, each threats has more than one interesting aspects to consider when ranking them. For example, natural disaster like earthquake happens with tremendous damage; however, it might not occur very often. In contrast, accidental threat like insulation failure happens comparatively often yet with limited damages. Heterogeneous natures and multiple characteristics of these threats make it difficult to compare them on the same scale with multiple considerations through conventional risk assessment measures. Therefore, it prompts the needs for a new framework and tool to rank them not only according to a single aspect but with most important considerations together.

In this paper, we developed a framework of finding the most imminent threats against the security of power system operation by ranking them, considering different aspects and their relationships among one another. The complicated ranking problem then can be treated as a multiple criteria decision-making problem. In further development, the Analytic Network Process (ANP) is employed to handle dependence and feedback in this complex decision process [3].

2. ANALYTIC NETWORK PROCESS

As a mathematical theory, the ANP was firstly introduced by Thomas L. Saaty in 1996 [3] to systematically handle dependence and feedback in a complex and conflict decision. The primary reason for introducing the ANP is to overcome the shortcoming of its precedent procedure AHP (Analytic hierarchy process), which is based on the functional independence of the upper parts from all their lower parts in the hierarchy, and from the criteria at each level [4]. However, not all problems can be expressed in a pure hierarchical fashion due to the interactions of various factors which may modify the importance of the weights on a global scale [5]. Therefore, Saaty suggested using AHP and ANP in different conditions. More specifically, when the alternatives or criteria are independent, AHP is highly recommended; while ANP can be used to solve the problem of dependence among alternatives or criteria [5].

The reason for ANP's success is that it provides a process to derive from qualitative judgments and quantitative measurements to ratio scale priorities for the influence among factors and groups of factors [6, 7].

ANP has been applied to many practical cases [8], mainly in economics and conflict resolutions, as well as in many engineering applications. Reference [9] employed ANP to determine the faulty behaviour risk in work system safety. Reference [10] combined group ANP, quadratic programming and interval preference information to develop a multi-criteria decision support system for improving civil defence and emergency management.

ANP is structured by using a series of pairwise comparisons to determine both the relative weights of each decision criterion and the rating of candidates (called alternatives/options) for each criterion. An analytic network model of a problem composes a set of clusters (i.e. groups of nodes), nodes (any aspect of the problem, e.g. alternatives, criteria etc.), and links (relationship and relative importance weights of different clusters and nodes inside).

Using ANP to solve a multi-criteria decision-making problem involves the following 4 steps:

1. Problem structuring and model construction,
2. Pair-wise comparison matrices and priority vectors,
3. Supermatrix formation and
4. Ranking or selection of the alternatives.

In the next section, we are going to discuss the ANP application to threats ranking in power systems and give an example of the threats ranking.

3. TRANSMISSION SYSTEM OPERATORS' PERSPECTIVE ON THREATS

To build a panorama of perceived threats on power system security in a specific region and on the transmission system operators' (TSOs) preparedness to respond the materialized threats, questionnaire was designed to gathering experts' feelings towards the threats in their own power system. The answers to the questionnaire are intended to be used to rank all of the threats using the Analytic network process (ANP) method.

In designing the questionnaire, as a considerable number of threats would be evaluated and the questionnaire survey is a "one-time-only" shot, we considered the wording for each item to be compact, accurate, easy to understand, and most importantly, short.

When considering the features of a threat, the most import ones are the severity of the impacts and the frequencies of its occurrence. These two factors would be essential for calculating its risk. For example, the power system is constantly at risk of becoming endangered by different threats, and in the case of threats materialization, consequences with different gravity will follow [11]. Common studies will take the frequencies of a threat times its damage for its risk. However, with the increase of preparedness, the caused damage can be diminished to some degree. Therefore, according to this consideration, we selected three most important features to describe a threat:

– *"likelihood to happen"*,

– *"impact gravity"*, and
– *"preparedness to respond"*.

For each of these features, we will ask transmission system operators' experts to score them on different scales by their personal judgment (Fig. 1).

More specifically, for the "*likelihood to happen*" of a threat, experts needed to mark it by an 11-scaled range from:

– *"0-never happened/won't happen"*,
– *"1-remotely maybe"* all the way to
– *"10 – frequent / extremely likely"*.

Similarly, experts will be asked to give his/her intuitive assessment on the "*impact gravity*" from

– *"0 - no impact at all"* to
– *"10 - extremely severe"*.

Unlike the first two features, the choices for answers to *"preparedness to respond"* were more specific, namely:

– *"0-Never heard of"*,
– *"1- Heard of"*,
– *"2- Not aware"*,
– *"3- Aware"*,
– *"4- About to analyze it"*,
– *"5- Already analyzed it"*,
– *"6- About to deploy countermeasures"*,
– *"7- Deploy countermeasures in progress"*,
– *"8- Already deployed"*.

questionnarie

The power system is constantly threatened by different threats. In the case of materialization of some threats on power systems, consequences will follow in different gravity. However, with the increase of the preparedness for them, the caused damage can be diminished to some degree. We would like to learn from your expertise and experience on *your opinion* toward these threats as an expert.

Please kindly to help us fill in the following questionnaire according to your insightful perspective. The answer does not need to necessarily reflect a precise analysis or your institutional official views, but rather express *your estimation* as an expert.

Instructions

For the evaluation of the likelihood, an 11-scaled mark is given from "0-Never happened" to "10-Frequently"; however, these terms are on a comparative term since the most frequent incidents happen in power systems are rear in common standards. The assessment of the impact for each threat is likewise based on an 11-scaled mark system, it should be evaluated in terms of their ability to cause blackouts. For those threats with '0-Never happend' do not necessarily suggest the impacts would also be '0-No impact at all', in such case, please give its impacts imagining it would happen in your grids.

Your Name:
Name of your company:

Questionnaire - Please evaluate the listed threats by choosing from the drop-off list

	THREATS		Likelihood in your network	The impact gravity	Preparedness to respond
Accidental threats	operational faults	design error	4	3	7- Deploy countermeasures in progress
		wrong decision	8	9	8- Already deployed
		maintenance accident	9	7	8- Already deployed
	equipments failures	technical failure	8	7	8- Already deployed
		animal interference	7	3	8- Already deployed
		defective maintenance or maintenance e	8	6	8- Already deployed
	fire threats	fire & explosions	6	8	8- Already deployed
	nuclear threats	nuclear disasters	0- Never happened	10- Extremely Severe	6- About to deploy countermeasures
	human threats	outsider threats	7	6	8- Already deployed
		social threats	1-remotely maybe	4	4- About to analyze it
Malicious threats	physical threats	terrorist attack	0- Never happened	9	7- Deploy countermeasures in progress
		war act	0- Never happened	10- Extremely Severe	7- Deploy countermeasures in progress
		random sabotage	1-remotely maybe	3	7- Deploy countermeasures in progress
	human threats	insider threats	1-remotely maybe	6	7- Deploy countermeasures in progress
	cyber threats	malware	4	4	8- Already deployed
		cyber-warfare and terrorists hacking	0- Never happened	4	7- Deploy countermeasures in progress
Natural Threats	geological disasters	avalanches	0- Never happened	0- No impact at all	0 - Never heard
		earthquakes	5	10- Extremely Severe	8- Already deployed
		volcanic eruptions	0- Never happened	0- No impact at all	0 - Never heard
		landslides	5	1	5- Already analyzed it
	hydrological disasters	floods	9	7	8- Already deployed
		limnic eruptions (lake overturns)	0- Never happened	0- No impact at all	0 - Never heard
		tsunamis	0- Never happened	0- No impact at all	0 - Never heard
	meteorological disasters	blizzards	10 - Frequently	8	8- Already deployed
		ice/hoar storm	9	7	8- Already deployed
		cold wave	6	6	8- Already deployed
		cyclonic storms	1-remotely maybe	5	6- About to deploy countermeasures
		droughts	8	5	8- Already deployed
		hailstorms	10 - Frequently	4	8- Already deployed
		heat waves	9	7	8- Already deployed
		tornadoes	1-remotely maybe	5	8- Already deployed
		lightning	10 - Frequently	3	8- Already deployed
		thunderstorm (electrical storm)	7	3	8- Already deployed
		rainstorm	10 - Frequently	6	8- Already deployed
	fires	wild fires	3	3	8- Already deployed
	health disasters	epidemics	0- Never happened	9	4- About to analyze it
		pandemics	0- Never happened	9	4- About to analyze it
		famines	0- Never happened	0- No impact at all	0 - Never heard
	space disasters	impact events	0- Never happened	10- Extremely Severe	0 - Never heard
		solar flares/solar winds/magnetic storms	0- Never happened	2	2- Not aware
	contamination	chemical & biochemical contamination	3	2	1- Heard of
		radioactive contamination	0- Never happened	5	5- Already analyzed it

Fig. 1. Questionnaire for TSO's perspective on threats (example).

The questionnaires in the example were filled in by an expert working with a TSO of the perceived threats on power system security for the trial purpose (not necessarily reflect his/her true opinion on the results).

Based on the trial answers given by the expert, we extend the scores to a pair-wise comparisons required by the ANP. Weight vectors, supermatirx and limit matrix were calculated to get the ranking of each threats according to a single criterion (Fig. 2) and the final ranking of the threats considering all aspects. Due to the sensitivities of the study, the final results are not given in this paper.

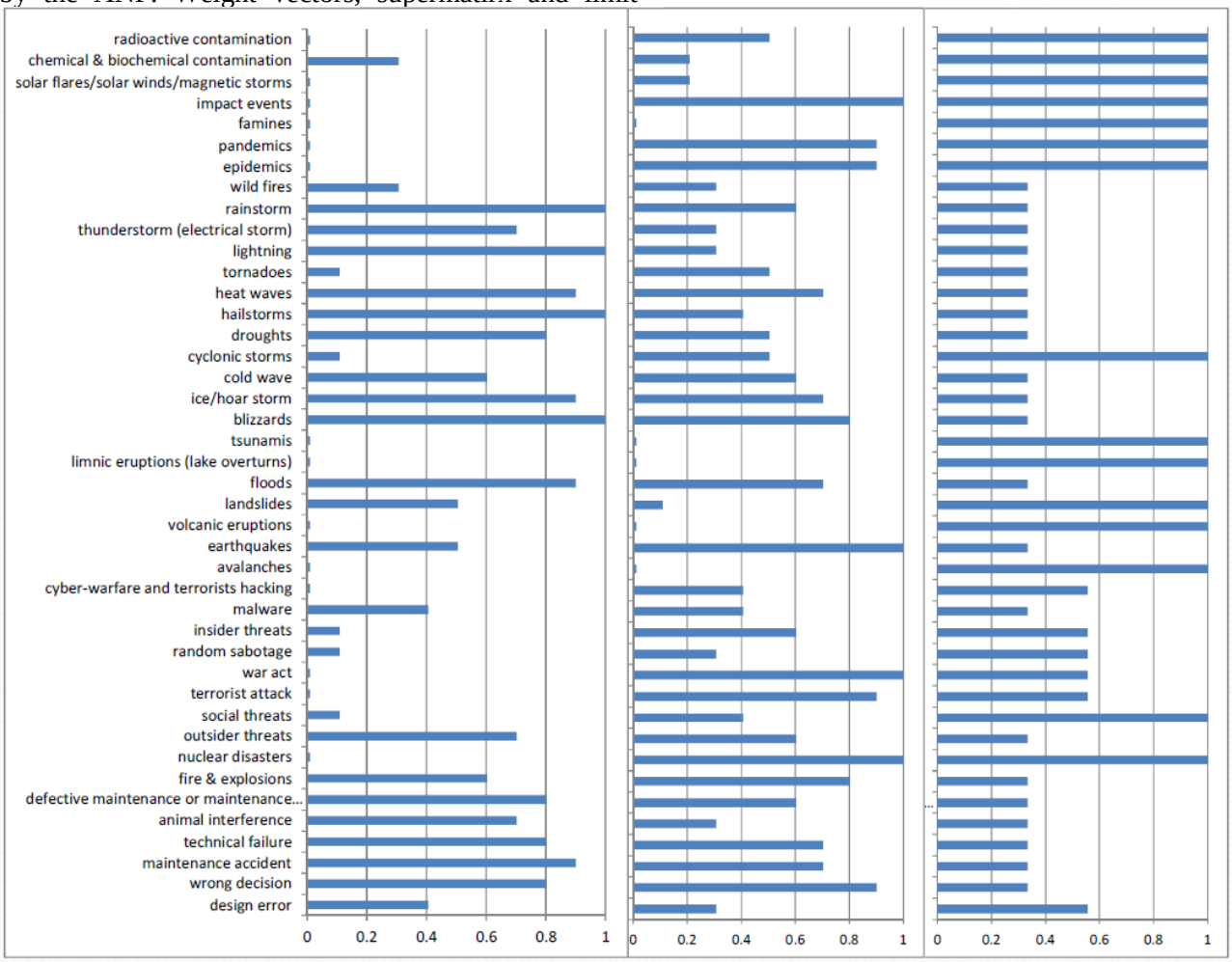

Fig. 2 Input evaluation for “likelihood”, “gravity”, “unpreparedness” (example).

5. CONCLUSION

Providing a panorama of all threats with different nature is quite a challenging task, especially when considering different features to outline them. Since the majority of traditional risk management methods are not suitable for considering threats with different natures at the same scale, further efforts are needed to develop a framework for qualitatively and quantitatively assessment of threats assessment, allowing ranking them with multiple criteria from a broader dimension like a group decision.

In this paper, we designed a framework for gathering the input for threats ranking and made a pilot trial by the approach. The results show that ANP is a suitable method for this purpose, and further extension seems to be promising for refine the results.

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] SESAME Project - Securing the European Electricity Supply Against Malicious and accidental thrEats, *Deliverable D1.2 Vulnerability and Threat Knowledge Base*, Version: 1.0, May 2012.

[2] **E. Bompard, T. Huang, Y. Wu**, *Classification and Trend Analysis of Threats Origins to the Security of Power Systems*, International Journal of Electrical Power & Energy Systems, 2013.

[3] **Thomas L. Saaty,** *Decision Making with Dependence and Feedback: The Analytic Network Process*, 4922 Ellsworth Avenue, Pittsburgh, PA: RWS Publications, 1996.

[4] **J.W. Lee and S.H. Kim**, Using analytic network process and goal programming for interdependent information system project selection. Computers & Operations Research, 2000. 27(4): p. 367-382.

[5] **Thomas L. Saaty**, The analytic network process. Decision Making with the Analytic Network Process, 2006: p. 1-26.

[6] **Thomas L. Saaty**, Lect9-ANP. ppt The Essentials of the Analytic Network Process with Seven Examples. Retrieved February, 2004. 10: p. 2008.

[7] **Thomas L. Saaty**, Theory and Applications of analytic network process. Vol. 4922. 2005: RWS publications Pittsburgh, PA.

[8] **R. Whitaker**, Validation examples of the analytic hierarchy process and analytic network process. Mathematical and Computer Modelling, 2007. 46(7-8): p. 840-859.

[9] **M. Dagdeviren, I. Yüksel, and M. Kurt**, A fuzzy analytic network process (ANP) model to identify faulty behaviour risk (FBR) in work system. Safety Science, 2008. 46(5): p. 771-783.

[10] **J.K. Levy and K. Taji,** Group decision support for hazards planning and emergency management: A Group Analytic Network Process (GANP) approach. Mathematical and Computer Modelling, 2007. 46(7-8): p. 906-917.

[11] **T. Huang, A. A. Purcărea, S. L. Voronca, M. Cremenescu, Y. Wu,** General overview on the societal and technical impacts of blackouts, Acta Electrotehnica Special Issue Proceedings of the 5th International Conference of Modern Power Systems MPS 2013, 28 – 31 May 2013 Cluj Napoca, Volume 54, Number 5, 2013, pag. 219 – 225, May 2013, Academy of Technical Sciences of Romania, Technical University of Cluj – Napoca, Romania, Institute of Electrical and Electronics Engineers Incorporated – Power & Energy Society, Romanian Section, Mediamira Science Publisher, ISSN 1841-3323.

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 2011 he has been working as WP leader, Executive Vice Coordinator (2012) on a FP7 project SESAME. 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, Romania
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 and is member in many Romanian and international professional associations such as International Council on Large Electric Systems CIGRE, WEC, EURELECTRIC.

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; has published 16 technical books and more than 80 articles and scientific papers.

Ying Jun WU, PhD
Polytechnic University of Turin, Department of Energy, Corso Duca degli Abruzzi, 24, 10129 Torino , Italy.
email: yingjun.wu@polito.it

Graduated at the Nanchang University, China, Electrical Engineering Faculty, study program – Power System. After finishing the university he started to study at the Southeast University, China, School of Electrical Engineering for his master's degree. PhD. graduated at the Politecnico di Torino, Italy, Energy Department, study program – Power Systems. His research topic is power system security and control.