

# Systemic Vulnerability of Swiss Power Grid to Natural Events

Amin abedi<sup>1</sup> and Franco Romerio<sup>1,2</sup>

<sup>1</sup>*Institute for Environmental Sciences, University of Geneva, Switzerland*

<sup>2</sup>*Geneva School of Economics and Management, University of Geneva, Switzerland*

**Abstract.** It is important to increase the security and robustness of power grids under a variety of events. In this case, “vulnerability analysis” is usually used to identify the most vulnerable elements of a power grid under different hazards. There are different kinds of methodology to identify vulnerability such as complex network, logical, functional methods and Monte Carlo simulation. In this work, the complex network, Swiss power grid, and seismic hazard are used as an approach, a test system, and a scenario, respectively. First, Swiss power grid is modeled using Gephi software and five different metrics of the complex network method are applied to the model. Then, TOPSIS as a multi-criteria decision method is used to combine the results of the previous step. Finally, to find out the most exposed nodes in the case of an earthquake, Swiss seismic hazard data is used and combined with TOPSIS outputs. The results show well the critical locations of power grid due to the seismic hazard.

## 1 Introduction

Today more than ever, electrical energy has become a key commodity to any growing society. Recent data show that climate change leads to increase number of extreme weather disasters, thus increasing the likelihood of severe impacts on power grid (big power outage, blackouts). In addition, many developments and changes in power grids such as decentralizing electricity generation, intermittent renewable generation and so on, might increase its complexity [1]. In USA, for example, the annual impact of weather-related blackouts ranges from \$20 to \$55 billion and the trend of such events shows that their frequency has increased over the last 30 years. Therefore, evaluating the robustness of critical infrastructures (CI) is mandatory to improve their design and control systems and reduce their vulnerability to unpredictable events [2].

“Vulnerability analysis” in power systems is important so as to determine how vulnerable a power system is in case of any unforeseen catastrophic events and is used to detect and rank the most critical elements of a power grid under a variety of scenarios such as natural disasters and so on [3].

There are different forms of vulnerability, including physical, social, organizational, economic, environmental, territorial and systemic vulnerabilities [4]. Among different type of vulnerabilities, physical and systemic vulnerabilities are more common in the risk and vulnerability analyses. Physical vulnerability represents the degree of loss of an element due to external pressure such as natural hazard while systemic vulnerability represents the degree of redundancy, functionality and dependency of an element in a system or the system as a whole due to failure of each element in the system or

failure of interconnected systems [5]. In this work, systemic vulnerability is focused on identifying the degree of redundancy, functionality and dependency of elements inside a power grid.

The goal of this work is to carry out a vulnerability analysis of the Swiss power grid and in particular:

- to determine the Swiss power grid’s inherent systemic vulnerability to a natural disaster to lessen the probability of a blackout,
- to identify the critical components, which in case of failure, could cause large consequences.

The rest of this report is organized as follows: first, used methodology and required data are introduced in section 2. Then, model of Swiss power grid is presented in section 2.4. Finally, in section 3, different results for vulnerability analysis of Swiss power grid are compared and systemic vulnerability of power grid due to seismic hazard is also presented. The conclusion will be provided in section 4.

## 2 Methodology and data

### 2.1 Complex network method

There are two different approaches for vulnerability analysis, analytical and simulation methods. Analytical methods can be categorized into topological and structural methods defined as complex network analysis (CNA), logical methods, functional methods and flow methods. Complex network methods are very fast and need few data while Monte Carlo methods are very slow, need many data, but have high accuracy. Characteristic of other

methods are between them. In this work, complex network analysis is selected because it is the fastest among them and can be achieved with the data at hand.

A network in CNA is composed of a set of nodes or vertices (in reality, substations or power plants in a power system) that are connected to each other by means of links or edges, e.g., power transmission lines in a power grid. In CNA, some metrics and indices (centralities) have been developed to identify that some nodes and edges are more critical or more important in a network than others are. The concept of centrality is from the idea that the closer a person to others is, the more important and critical information he/she holds. In turn, he/she has more power, and greater influence [2].

In purely complex network analysis, the basis is the mapping of buses and transmission lines of power grids to nodes and edges, respectively. The defined centralities in complex network theory are used to analyze their vulnerability. Metrics and centralities in complex network theory can be divided into two groups. The first one calculates the closeness of nodes/edges to each other such as degree and closeness centralities. The second group is based on how nodes/edges stand between the others, for instance, efficiency (shortest-path) or flow betweenness centralities. However, there are other centralities that combine two above mentioned ideas such as delta centrality (or  $\Delta$  centralities) and combined degree-betweenness centrality [6].

**Degree:** degree probability distribution can show topological features of a network.

$$\frac{\sum a_{ij}}{N-1} \quad (1)$$

**Closeness:** closeness centrality is defined as the sum of all its shortest paths and can be used to quantify how rapidly the information injected in each node spreads in the network [7].

$$\frac{N-1}{\sum d_{ij}} \quad (2)$$

**Betweenness:** betweenness measures the ratio and total number of shortest paths in a graph and as a result, nodes with high values of the metric can be designated to control or regulate information flowing within a network [7].

$$\frac{1}{(N-1)(N-2)} \sum_{i \neq j \neq k} \frac{n_{jk}(i)}{n_{jk}} \quad (3)$$

**Eigenvector Centrality:** The eigenvector centrality is based on the idea that a node is important if it is connected to other important nodes [8].

$$\frac{1}{\lambda} \sum_{j=1}^N W_{ij} e_j \quad (4)$$

**PageRank (PR) algorithm:** The essence of PR algorithm is that the rank of a node will be certainly high if the node is linked from a high-ranked one [9].

$$\frac{1-q}{N} + q \sum_{D_{in}(p_i)} \frac{PR(p_j)}{D_{out}(p_j)} \quad (5)$$

Where in (1-5):  $G$  is the graph descriptive of the structure of the real network with  $N$  nodes,  $i, j, k \in G$ .  $a_{ij}$  is 1 if node  $i$  is connected to node  $j$ .  $d_{ij}$  is the shortest path from node  $i$  to node  $j$ ;  $n_{jk}(i)$  is the number of shortest paths that contain  $i$ ;  $n_{jk}$  is the number of shortest paths from node  $k$  to node  $j$ .  $\lambda$  and  $W_{ij}$  are a constant and weight respectively.  $q$  is the damping factor, which would be set to 0.85, and  $D$  is equal to the number of the directed transmission lines.

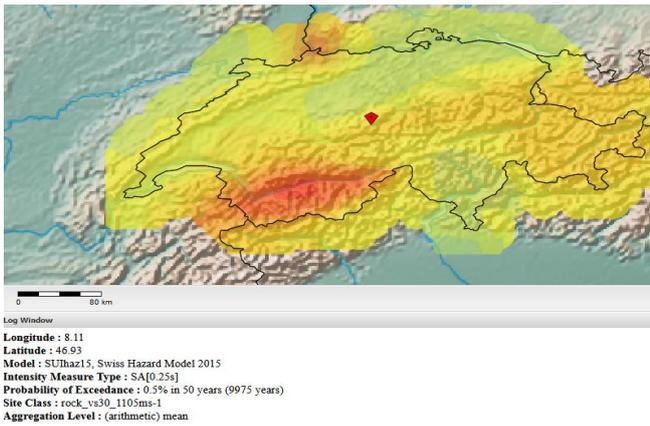
## 2.2 Multi-criteria decision methods (MCDM)

For vulnerability and risk analyses of complex networks, there is no holistic analysis to integrate the structural, static, dynamic, operational features and complexity of these networks and instead, the so-called reductionist methods are proposed such as complex network methods, power flow methods, logical methods, functional methods and Monte Carlo simulation. So, important or critical measures (indices) based on different definitions lead to different ranking results. Therefore, these results should be combined with approaches such as multi-criteria decision methods (MCDM) and provide a unique ranking from different measures to be useful for decision makers. The Technique for Order Preferences by Similarity to an Ideal Solution (TOPSIS) is one of the MCDM to find a best alternative that is the closest to the positive ideal solution and farthest to the negative ideal solution [10]. In this work, TOPSIS is used to combine different complex network metrics introduced in the previous subsection.

## 2.3 Required data

According to reference [1], earthquakes, storms, floods, landslides and heat waves are among the major causes of electricity blackouts during natural disasters. These events can destroy or damage the electrical infrastructures and trigger cascading effects. Earthquake is one of the most important hazards that can affect different parts of power system such as nodes (generator, transformers, substation and control centers) and edges (overhead line and cables). It should be noted that in each country one of natural hazards are the major according to historical records and based on their frequency and impacts. Storms are more frequent in Switzerland but earthquakes are more costly [11], herein, seismic hazard is selected as our scenario.

The data on seismic hazard for Switzerland and its assumptions (see Figure 1) is provided by European Facilities for Earthquake Hazard and Risk (EFEHR) [12]. Spectral Acceleration (SA) is approximately what is experienced by a building during earthquakes. Short buildings (less than 7 stories) have short natural periods (0.2 to 0.6 sec) [13]. Buildings and structures in our case (substations and transformers) are usually in this category and have heights less than 2 stories tall. That is why 4 Hz (0.25 s) is selected for this goal. In addition, the choice of return period depends on the importance of the structure for the functioning of the society. Because a power grid is one of the most important infrastructure, one needs to consider the highest return period as it provides the



**Figure 1.** Swiss seismic hazard map and its assumptions.

highest level of expected spectral acceleration the infrastructure will be submitted to.

### 2.4 Swiss power grid modelling

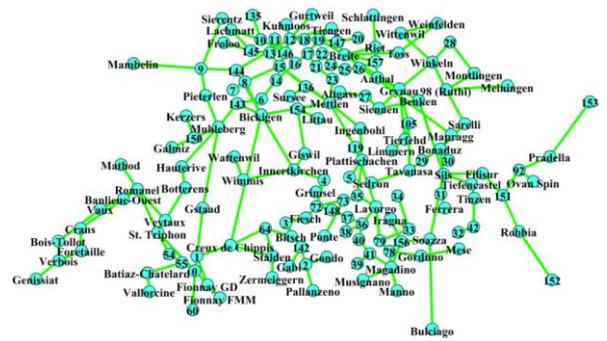
The power grid topology is achieved from comparing Openstreetmap website [14], the Swiss transmission grid operator (Swissgrid), google map, Over-Turbo website [15] and map of European Network of Transmission System Operators for Electricity (ENTSOE) [16]. The georeferenced model based on the Swiss transmission system is plotted using Gephi (an open source software) [17] in Figure 2.

## 3 Results

Data gathering and modelling of power grid (the nodes that can be substations, power plants, etc. and the lines are assumed a straight line between nodes) are discussed in the previous sections. In this section, the modelled grid is used and at first, the five centralities for this topology are calculated. Table 1 shows top five important nodes in Swiss grid using different metrics.

As shown in Figure 3 and Table 1, the results are not exactly the same because of different definitions and criteria used for the analysis. For instance, Node 12, located north of Switzerland, is the most important node according to three metrics, while for the last two metrics; it appears at the 3rd and 4th rank. The node Mettlen is another example, being at the 2nd rank for 4 metrics, and 1st in one metrics.

Therefore, depending on the criteria (indices) used, the analysis leads to different ranking results. So, these results should be combined with approaches such as MCDM in order to provide a unique ranking from different measures to be useful for decision makers. Herein, TOPSIS is used to combine different complex network metrics calculated above. Figure 3f and Table 2 show the results of TOPSIS. According to the results, node Mettlen is the most important and critical node in Swiss power grid without considering its environment. The magnitudes in this figure are TOPSIS results and are dimensionless. In Figure 3, the more one (bigger circle) is the more vulnerable node.



**Figure 2.** Georeferenced model based on the Swiss transmission system is plotted using Gephi.

Finally, we need to consider the position of nodes in relation to seismic hazard to define what would be the most exposed nodes in case of earthquakes. In order to achieve this task, hazard data were extracted using ArcMap software from downloaded shape-file are combined by multiplying the value of the spectral acceleration as a weight with the value obtained from the TOPSIS analysis using MATLAB programming. As shown in Table 3, node “Creux de Chippis” is the most node at risk in Switzerland when considering seismic hazard. Figure 4 shows the most critical nodes in regards with seismic hazard.

**Table 1.** Top five important nodes using different metrics

Rank	Degree	Closeness	Betweenness	Page Rank	Eigenvector
1	12	Mettlen	Bickigen	12	12
2	Mettlen	Bickigen	Mettlen	Mettlen	Mettlen
3	Breite	12	Chippis	Breite	19
4	Bickigen	144	12	Sils	15
5	19	15	Sils	Magadino	Breite

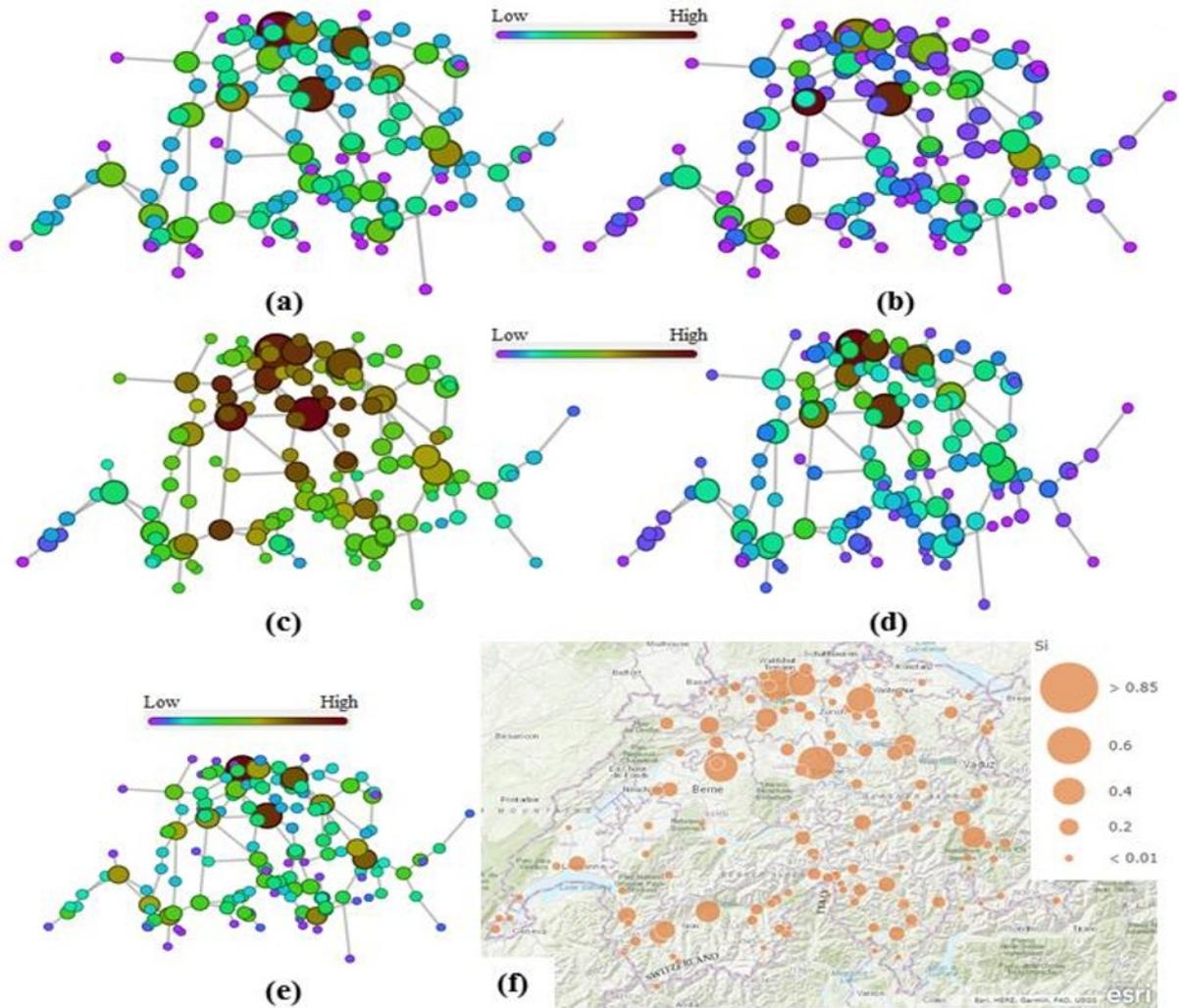
**Table 2.** Top five important nodes using TOPSIS

Label	D+	D-	S <sub>i</sub>	Rank
Mettlen	0.017	0.103746	0.859205	1
12	0.028848	0.103048	0.781281	2
Bickigen	0.030411	0.10054	0.767766	3
Breite	0.04635	0.076886	0.623891	4
19	0.047667	0.077388	0.61883	5

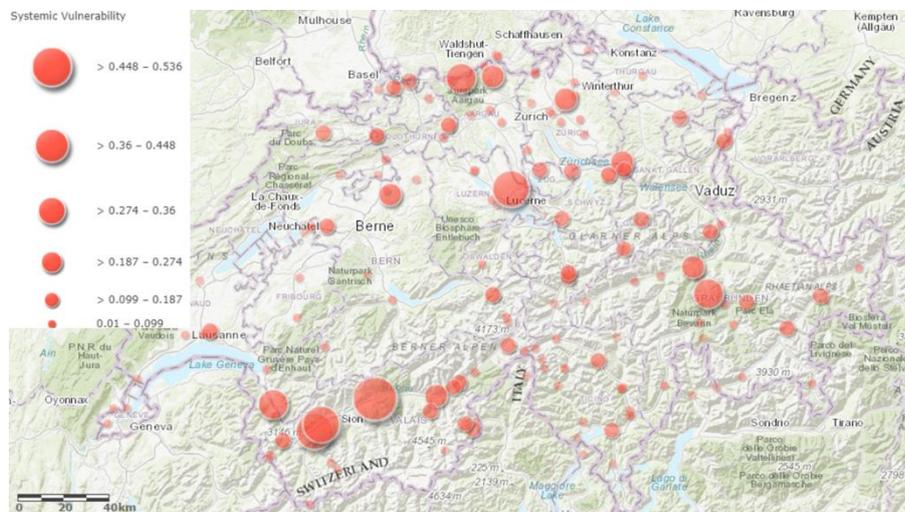
D+ and D-: Distance between alternatives and the positive and negative ideal solutions, respectively, S<sub>i</sub>: relative closeness to the positive and ideal solution.

**Table 3.** Top five important nodes to seismic hazard

Node Label	Latitude	Longitude	Systemic Vulnerability	Rank
Creux de Chippis	46.28685	7.55782	0.536147	1
0	46.15828	7.20941	0.417621	2
1	46.18547	7.24901	0.410494	3
Mettlen	47.1154	8.33728	0.369693	4
12	47.54997	8.04951	0.339473	5



**Figure 3.** Vulnerability analysis of Swiss power grid (nodes) using (a) degree definition, (b) betweenness centrality, (c) closeness centrality, (d) eigenvector centrality, (e) PageRank centrality and (f) combining different complex network metrics using TOPSIS. Numbers are dimensionless. The higher the value, the more vulnerable the node is.



**Figure 4.** Systemic vulnerability of Swiss power grid due to seismic hazard.

## 4 Conclusion

“Vulnerability analysis” of power systems is used to detect and rank the most critical elements of a power grid under a variety of attack scenarios. On the other hand, the robustness of CIs must be evaluated to improve their design and control systems, and to reduce the vulnerability to unpredictable events.

In this work, the main goal was calculation of vulnerability in Swiss power grid. So, it is modelled using Gephi and five different measures of complex network method such as degree, betweenness, closeness, PageRank, eigenvector centralities are calculated. Then, these measures are combined using TOPSIS method and a unique importance ranking is calculated. These results are then combined with seismic hazard to identify the more exposed nodes.

It is shown that important and critical nodes are different for different scenarios. Node “Creux de Chippis” is the most important node in Switzerland due to seismic hazard while node Mettlen is the most important and critical node in Swiss power grid without considering their environment.

## Acknowledgment

We would like to express our very great appreciation to Dr Corine Frischknecht for her valuable and constructive suggestions during the planning and development of this research work. We would also like to extend our thanks to CERG-C lecturers and organizing committee.

## References

1. Komendantova, N., et al., *Protecting Electricity Networks from Natural Hazards*. 2016, Organization for Security and Cooperation in Europe (OSCE).
2. Abedi, A., L. Gaudard, and F. Romerio, *Review of major approaches to analyze vulnerability in power system*. Journal: Reliability Engineering and System Safety (in press).
3. Kröger, W., E. Zio, and M. Schläpfer, *Vulnerable systems*. 2011, London: Springer. xiv, 204 pages.
4. Dolan, M., et al., *Forensic Disaster Analysis of Flood Damage at Commercial and Industrial Firms*, in *Flood Damage Survey and Assessment*. 2017, John Wiley & Sons, Inc. p. 195-209.
5. Veen, A.V.D. and C. Logtmeijer, *Economic Hotspots: Visualizing Vulnerability to Flooding*. Natural Hazards, 2005. **36**(1): p. 65-80.
6. Guan, X., et al. *Power grids vulnerability analysis based on combination of degree and betweenness*. in *The 26th Chinese Control and Decision Conference (2014 CCDC)*. 2014.
7. Gutierrez, F., et al., *Vulnerability Analysis of Power Grids Using Modified Centrality Measures*. Discrete Dynamics in Nature and Society, 2013.
8. Liu, B., et al., *Recognition and Vulnerability Analysis of Key Nodes in Power Grid Based on Complex Network Centrality*. IEEE Transactions on Circuits and Systems II: Express Briefs, 2017.
9. Li, C., et al. *Method for evaluating the importance of power grid nodes based on PageRank algorithm*. IET Generation, Transmission & Distribution, 2014. **8**, 1843-1847.
10. Behzadian, M., et al., *A state-of-the-art survey of TOPSIS applications*. Expert Systems with Applications, 2012. **39**(17): p. 13051-13069.
11. Huang, T., et al., *Analysis and Visualization of Natural Threats Against the Security of Electricity Transmission System*, in *The Scientific Bulletin of Electrical Engineering Faculty*. 2017.
12. *European Facilities for Earthquake Hazard and Risk*. 2018; Available from: <http://www.efehr.org/en/hazard-data-access/Intro/>.
13. *Earthquake Hazards Technical Q&A*. 2018 [20.04.2018]; Available from: <https://earthquake.usgs.gov/hazards/learn/technical.php>.
14. *openstreetmap*. Available from: <https://www.openstreetmap.org>.
15. *Over-Turbo website* 2018; Available from: <https://overpass-turbo.eu/>.
16. *European Network of Transmission System Operators for Electricity* 2018; Available from: <https://www.entsoe.eu/map/Pages/default.aspx>.
17. Bastian, M., S. Heymann, and M. Jacomy, *Gephi: An Open Source Software for Exploring and Manipulating Networks*. 2009.