Electrical Power and Energy Systems 78 (2016) 436–444

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

# A knowledge based decision support algorithm for power transmission system vulnerability impact reduction

Ersen Akdeniz [a,*], Mustafa Bagriyanik [b]

[a] TUBITAK Marmara Research Center, Energy Institute, Gebze, Turkey
[b] Istanbul Technical University, Department of Electrical Engineering, Istanbul, Turkey

ARTICLE INFO

*Article history:*
Received 24 July 2015
Received in revised form 9 October 2015
Accepted 17 November 2015
Available online 23 December 2015

*Keywords:*
Power system vulnerability analysis
Non-operational vulnerability indices
Fuzzy inference system
Knowledge based decision support algorithm

ABSTRACT

One of the main reasons for wide area blackouts is cascading failures due to critical contingencies. Since, several factors such as faults, misoperations, environmental effects and sabotage issues are involved; the analysis of such contingencies is a challenging process. Most available methods in literature deal mainly with a certain aspect of the problem. In this study, a more comprehensive methodology using operational and non-operational indices for power system vulnerability analysis is presented. The individual indices are defined for power system's operational performance, terrorist attack and adverse weather conditions where a fuzzy inference system is used to obtain a single Total Vulnerability Index for each transmission system line. Additionally, a knowledge based decision support algorithm is proposed for the use of TSO's defense activities in order to determine the weak points and counter measures like load shedding. The modeling approach is tested on IEEE reliability test network with imposed external constraints.



## Introduction

According to the recent reports, electricity consumption has increased above forecasts in many countries while power industry is still having a restructuring process where the main driving force is profit maximization [1]. Contrary to this fact, the transmission network investments have not increased in parallel with the demand growth mostly due to political, economic and environmental reasons. As a result, most of the power systems are kept operated close to their operational limits, yielding a vulnerable operation. This vulnerability has been confirmed by recent large-scale events involving the outage of multiple system components [2].

The term vulnerability is defined as; "manifestation of the inherent states of the system that can be exploited by an adversary to harm or damage the system" [3]. In literature, power system vulnerabilities are traditionally discussed from the resulting impacts side such as loss of load regarding stability and contingency [4,5]. In [6,7] the subject is studied from the perspective of environmental impacts while there are several studies discussing vulnerabilities in the form of terrorist attack problem formulized as a bi-level optimization regarding physical and cyber threats [8–10]. From the network theory side [11] there approaches for finding potential bottlenecks, however in [12] it is indicated that such approaches are not practical since capacity constraints are not considered. Also, in [13] a Probabilistic Risk Analysis (PRA) is used for power systems equipment ranking where the impacts are analyzed in a detailed manner considering economical and public issues for which the constructed performance scales are derived from inputs provided by different stake holders. Since, the importance of each impact is obtained from different available stakeholders; the results may not be globally applied unless supported by a common data base. In [14,18,23] operational indices are combined with environmental impacts, but a more comprehensive way of vulnerability analysis dealing with all aspects of the problem is still needed.

Within the scope of this paper, power transmission system vulnerability indices are clearly defined as operational and non-operational groups. Assuming the test system is at steady state after loss of any transmission line, operational vulnerability rankings for each line is obtained. Then, considering mainly terrorist attack and adverse weather constraints non-operational indices are calculated. Using a Fuzzy Inference System (FIS) for total vulnerability evaluation is obtained in order to have a figure of merit for global vulnerability analysis of power system. Finally, using these indices a Knowledge Based Decision Support Algorithm (KBDSA) is discussed which can assist Transmission System Operator (TSO)'s for early detection of cascading failures in terms of intelligent load shedding during probable power system incidents.

* Corresponding author.

http://dx.doi.org/10.1016/j.ijepes.2015.11.041
0142-0615/

**Nomenclature**

*Indices*

| | |
|---|---|
| $l$ | line index |
| $i$ | bus index |
| $g$ | generator index |

*Constants*

| | |
|---|---|
| $n_{line}$ | total number of lines |
| $n_{bus}$ | total number of buses |
| $n_{gen}$ | total number of generators |
| $N$ | formulation parameter |
| $w_P$ | overloading weight factor |
| $w_b$ | bus voltage weight factor |
| $w_g$ | generator reactive power weight factor |
| $L_l$ | length of $l^{th}$ line |
| $L_{max}$ | Max. value of line lengths |
| $MVA_l$ | MVA capacity of $l^{th}$ line |
| $MVA_{max}$ | maximum value of line MVA capacities |
| $w_{cap,l}$ | relative line MVA capacity |
| $w_{ll,l}$ | line length ratio of $l^{th}$ line |
| $w_{vcd,l}$ | relative vertical clearance distance to ground ratio |
| $w_{gl,l}$ | geographical vulnerability level |
| $w_{pr}$ | priority percentage weight factor |
| $w_{ws,l}$ | weather state vulnerability level |
| $D_{vl1}$ | vertical clearance distance to ground for voltage level-1 |
| $D_{vl2}$ | vertical clearance distance to ground for voltage level-2 |

*Variables*

| | |
|---|---|
| $P_l$ | active power of $l^{th}$ line |
| $P_{l\text{-}max}$ | max active power of $l^{th}$ line |
| $V_i$ | voltage level of $i^{th}$ bus |
| $V_{bc}$ | base case voltage of $i^{th}$ bus |
| $V_{min}$ | minimum voltage of $i^{th}$ bus |
| $V_{max}$ | maximum voltage of $i^{th}$ bus |
| $C_i$ | $i^{th}$ bus consumption |
| $C_{tot}$ | total consumption |
| $G_i$ | bus generation |
| $G_{tot}$ | total generation |
| $w_{sl,i}$ | $i^{th}$ bus security level |
| $w_{pl,i}$ | $i^{th}$ bus protection level |
| $w_{sc,i}$ | $i^{th}$ bus social criticality impact |
| $R_{PO,l}$ | line physical openness level |
| $R_{ta,i}$ | $i^{th}$ bus terrorist attack vulnerability level |
| $w_{size,i}$ | power generation & consumption level of $i^{th}$ bus |
| $R_{TA,l}$ | total terrorist attack vulnerability of $l^{th}$ line |
| $R_{TA,ij}$ | $l^{th}$ line terrorist attack due $i^{th}$ and $j^{th}$ buses |
| $PI_P$ | active power performance index |
| $PI_V$ | voltage performance index |
| $R_{OP,l}$ | operational performance vulnerability of $l^{th}$ line |
| $R_{AW,l}$ | adverse weather vulnerability of $l^{th}$ line |
| $R_{IF,l}$ | internal failure vulnerability of $l^{th}$ line |
| $\lambda_n, \lambda_s, \lambda_m$ | failure rates for normal, severe and moderate weather condition |
| $T_n, T_s, T_m$ | time periods for normal, severe and moderate weather conditions |

## Vulnerability indices

Having almost the same network built several decades ago, the system operators have to cope with today's challenges arising from increased consumption, increasing penetration of distributed resources, climate changes and ageing [15]. In order to have proper level of serviceability, an acceptable level of vulnerability must be guaranteed within the power system. A common way to have an aggregated vulnerability evaluation employed by system operators and the related academicians are involved in contingency screening methods mainly dealing with operational parameters [16,17]. Additionally, the fault statistics are used as the main source of vulnerability measure. However, most wide area spread blackouts are triggered by adverse weather conditions or terrorist attacks for which very limited information is available [18]. Considering that electrical parameters are also affected by several external factors and the available statistical information actually contains already failed components statistics, a comprehensive method is needed to have a more precise vulnerability degree evaluation. Power transmission system vulnerabilities can be grouped in two main groups as operational and non-operational indices as seen in Fig. 1. While operational performance indices focusing on internal and mostly electrical performance measures, non-operational indices mainly deals with possible and probable risks associated with external conditions and cases which cannot be controlled by TSOs. Although, the vulnerability indices can change according to the TSO's experience and specific conditions, in order to present a generalized figure of merit for power system vulnerability analysis, steady state operational limits for contingency impact analysis are considered as the operational performance indices. The dynamic and transient stability issues are not considered at this stage due to a need for time-varying dynamic system model. For the non-operational indices, Terrorist Attacks (TA), Adverse Weather (AW) and Internal Failures (IF) are considered basically. Although, internal failures are directly related with power system equipment itself, due to uncertainty factor, it is considered in non-operational performance indices in this study.

### *Operational performance indices*

In terms of operational performance indices, only steady state stability limits are taken into consideration due to modeling limitations. As given in [19], active power performance index (1) is used as an indicator for thermal loading level of lines and voltage performance index (2) is employed for bus voltage stability considering deviations from base case together with reactive power loading variations of generators.

$$PI_P = \sum_{l=1}^{n_{line}} \frac{w_P}{2} \left( \frac{P_l}{P_{l-max}} \right)^{2N} \tag{1}$$

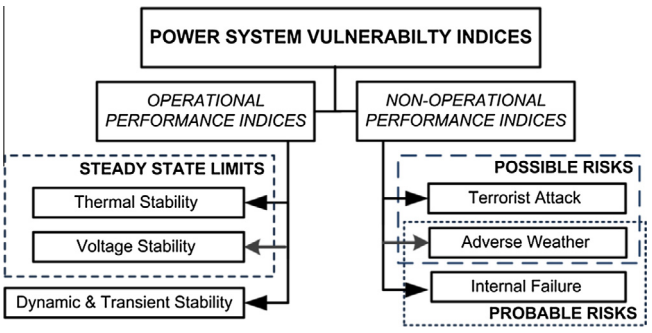


**Fig. 1.** Power system vulnerability indices.