A New Approach for Terrorist Attack Vulnerability Evaluation of Power Transmission Lines

Ersen Akdeniz[1], Mustafa Bağrıyanık[2]

[1]TUBITAK MRC Energy Institute, P.K.:21 41470, Gebze, Turkey
ersen.akdeniz@tubitak.gov.tr
[2]Istanbul Technical University, Department of Electrical Engineering, Istanbul, Turkey
bagriy@itu.edu.tr

Abstract

Power transmission systems are prone to several vulnerabilities which may result in deterioration of system stability and incapacities due to equipment contingencies. The causes leading to contingency and instability are ranging from natural disasters to malevolent acts as well as misoperations and equipment's hidden failures. In principle, most power systems are designed in an efficient manner in order to provide openness and accessibility for Transmission System Operator (TSO) personnel. As a result of this fact, the term power system vulnerability becomes directly related with the physical reach of either natural calamities or some terrorist acts. Thus, a measure for possible disruption events is needed in order to have a more generalized and comprehensive figure of vulnerability degree measurement required for analysis. In this study, a measure for power transmission line's terrorist attack vulnerability evaluation is presented using IEEE reliability test system with external constraints imposed on system data.

1. Introduction

Recent wide area blackouts reveal that today's so called modern society is heavily depended on service continuity of electricity [1]. Although, technological improvements reached a tremendous pace, the electricity supply systems rather slowly adapted and upgraded due to fact that they are already being spread out and customers have a strong desire for service continuity. However, having almost the same network whose several parts dating several decades ago, the system operators have to cope with today's challenges arising from increased consumption, increasing penetration of distributed resources, abnormal climate changes and ageing of course [2]. In order to have proper level of serviceability, an acceptable level of vulnerability must be guaranteed within the electricity system. With the help of vulnerability analysis results, TSO's can improve their emergency preparedness. While off-line vulnerability analysis can guide investments and maintenance priority plans, on-line vulnerability analysis provide assistance for load dispatchers in optimizing system load-frequency control actions and improve survivability levels after faults affecting a wide area of the electricity system.

Considering vulnerabilities for power systems, the disruption leading vulnerability may arise either from internal operational causes or impacts arising from external conditions. Also, another issue that also must be taken into consideration is the intention factor; such as the root cause of the incident. The source of disturbance can be either due to an accident and malfunction of a component or some deliberate acts yielding abnormal operation. As, more scenarios are included, it turns out that power system vulnerability analysis is not only a technical analysis in terms of contingency and stability, but also have some additional environmental and sociological features that are to be included in the optimal solution. By doing so, TSO's will have a broader understanding of the emergency conditions and can have the chance to adapt their defense strategies according to the type of the disturbance.

In literature, several studies discuss power system vulnerability issue as terrorist attack problem formulized in the form of a bi-level optimization mainly focusing on the final impacts on power network, such as loss of energy (LoE) or loss of generation (LoG) [3]-[6]. However, the selection criteria of targets is mainly based on power flow level (ie, selecting maximum power transferred/loaded lines) which is almost independent from the physical and environmental factors of the transmission system itself. Also, acting behavior of the terrorist attacks should be taken into consideration in terms of distribution of work force capability and intellectual level of system knowledge.

Within the scope of this study, a numerical evaluation approach for terrorist attack vulnerability ranking of transmission system lines is aimed to be presented. In section 2, the detailed description of the problem is made. In section 3, the mathematical definition and evaluation methodology is presented. In section 4, the simulation results using IEEE reliability test system are given. Finally, the conclusions are presented in section 5.

2. Problem Description

According to the occurrence nature of the disturbance, the risks that can be estimated from historical data are regarded as probabilistic risks whereas for the threats which are possible to happen and does not have a statistical data should be evaluated. In terms of attack type, terrorist acts can be classified as; direct physical attacks, direct cyber-attacks and insider impacts which support the intruder agents by eliminating physical or cyber barriers. The insider personnel can physically disable the firewall units or inject a Trojan virus just by connecting a USB memory stick to internal LAN even if the system has no remote access. Also, if the insider has a direct access to surveillance control system may deactivate the fences or locked door systems by which in turn can let the intruders have direct access to facility. In principle, three main types of malevolent acts and / or

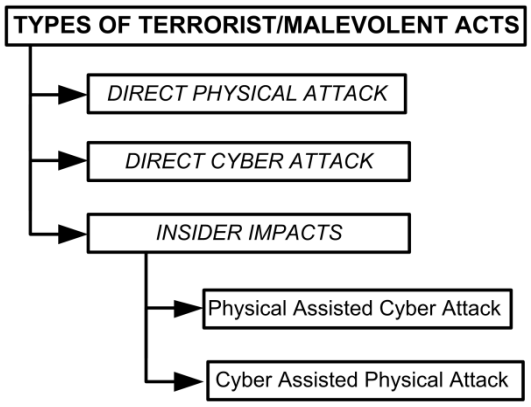

Fig.1. Classification of terrorist attacks on power systems

sabotages upon power systems are described as terrorist attacks which are seen in Fig.1. Accordingly, the total terrorist attack vulnerability can be expressed as follows;

$$V_{TA} = f\{V_{P.A,d,}\,;\, V_{P.A,i}\,;\, V_{C.A,d}\,;V_{C.A,i}\} \qquad (1)$$

where, $V_{P.A,d}$, $V_{C.A,d}$ are direct physical and cyber-attack vulnerability and the insider impacts are described as $V_{P.A,i}$, $V_{C.A,i}$ reflecting indirect components affecting physical and cyber-attack vulnerability, respectively. But, the determination of these vulnerabilities is not so easy due to lack of historical data especially for the insider impact and possible correlation of the defined parameters. However, the cumulative attraction and the accessibility of the targets are the main criteria for the intruder agents. So, we can at least determine a measure for vulnerability ranking of transmission lines in terms of terrorist attack. While the size and social criticality determines attractiveness, the level of protection and physical openness determines the direct accessibility level of the target for the intruder [7]. Knowing that power transmission system's electrical parameters are also affected by several external factors and the available statistical information actually contains already failed components statistics, another point of view including several vulnerability indicators is needed in order to have a more broader vulnerability degree evaluation of the grid. While operational performance indices focusing on internal and mostly electrical performance measures, terrorist attack vulnerability indices mainly deals with possible and probable risks associated with external conditions and cases which are located at indirect reach of power system operators. It should be remembered that the vulnerability indices can change according to the TSO's experience and specific conditions of each electrical system, thus several other indices can be defined as non-operational indices influencing power system vulnerability.

It is very critical for the TSO to determine the main cause of interruption in order to improve the emergency preparedness of the system. As the root cause of the disturbance is determined as terrorist attack, the TSO's system defense plan can be updated accordingly. If the impact is tolerable within the system reserves, short term activities including load shedding, line switching and increase in active power generation methods are employed. Otherwise, if the post-fault recovery seems impossible, partial islanded mode operation methods might be employed.

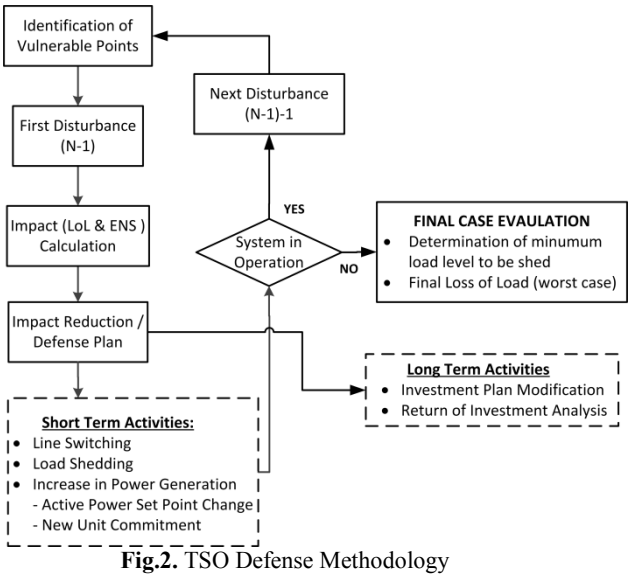

Fig.2. TSO Defense Methodology

In the scope of long term impact reduction activities, new investment plans regarding improvement of redundancy and capacity of power network should be employed. At this point a return of investment analysis is required considering direct and indirect energy costs. The generalized TSO defense methodology is presented in Fig.2.

3. Evaluation Methodology

In this study, a vulnerability measure for transmission system lines and buses are studied. The overall terrorist attack vulnerability ranking of lines is composed of two main components, one is sourcing from physical characteristics of the system and the other is due to the importance level of the connected buses. In order to calculate a measure for terrorist attack indices for lines; the summation of physical openness level of the lines and attack vulnerability of the connected buses (which are connected by the individual line) are used. Also, the relative length of lines, the relative vertical clearance distance to ground of lines [8] and the individual line's MVA capacity are used to characterize physical openness and accessibility for terrorist attacks. Similarly for buses, the protection level, the social criticality level and the percentage of power generation and consumption of the buses connected by the individual line are defined as a measure for attraction and accessibility. The calculation details of overall terrorist attack vulnerability of lines, $V_{TA,l}$, is described as follows;

$$V_{TA,l} = V_{PO,l} + V_{TA,bus} \qquad (2)$$

$$V_{PO,l} = w_{ll,l} * w_{vcd,l} * w_{cap,l} \qquad (3)$$

$$V_{TA,bus} = V_{ta,i} * V_{ta,j} \qquad (4)$$

$$V_{ta,i} = w_{pl,l} * w_{sc,i} * w_{size,i} \qquad (5)$$

$$w_{ll,l} = \frac{L_l}{L_{max}} \qquad (6)$$

$$w_{vcd,l} = \frac{D_{vl_1}}{D_{vl_2}} \qquad (7)$$

$$w_{cap,l} = \frac{MVA_l}{MVA_{max}} \qquad (8)$$

$$w_{size,i} = \frac{C_i}{C_{tot}} + \frac{G_i}{G_{tot}} \qquad (9)$$

where,

L_l : length of l^{th} line

L_{max} : the longest line's length

D_{vl1}, D_{vl2} : vertical clearance distance to ground for different voltage levels (1&2)
C_i : i^{th} bus consumption
C_{tot} : total consumption
G_i : i^{th} bus generation
G_{tot} : total generation
MVA_l : MVA capacity of l^{th} line
MVA_{max} : maximum value of line MVA capacity
$w_{ll,l}$: relative line length ratio of l^{th} line
$w_{vcd,l}$: relative vertical clearance distance to ground ratio
$w_{cap,l}$: relative line MVA capacity
$w_{size,i}$: power generation and consumption level of i^{th} bus
$w_{sl,i}$: i^{th} bus security level
$w_{pl,i}$: i^{th} bus protection level, $(1-w_{sl})$
$w_{sc,i}$: i^{th} bus social criticality impact
$V_{PO,l}$: line physical openness level
$V_{ta,i}$: i^{th} bus terrorist attack vulnerability level
$V_{TA,bus}$: l^{th} line terrorist attack component due i^{th} and i^{th} buses
$V_{TA,l}$: total terrorist attack vulnerability of l^{th} line

The equivalent bus protection level, w_{pl}, is considered to be complementary to the security level value of the individual bus. Regarding public opinion, the impact degrees of social criticality factors are given in Table.1 [9]. According to the security level descriptions given in Table.2 [10] the buses are assigned with the corresponding security level. Using the above defined parameters terrorist attack vulnerability measures for lines and buses are calculated. In this study, in order to calculate the terrorist attack vulnerability of the test system, below assumptions on physical and environmental constraints of test system are made;

- Generator buses have the highest security and lowest physical access level,
- Load buses have the lowest security and highest physical access level,
- The lines are considered equally vulnerable in terms of cyber-attack and the relevant bus's cyber vulnerability is directly associated with the security level.

Table 1. Social Criticality Level Distribution

Order	*Security level*	*Degree*
4	Severe	1.0
3	High (H)	0.8
2	Moderate (M)	0.5
1	Low (L)	0.2

Table 2. Security Level Distribution

Order	*Security level*	*Description*	*Degree*
6	Extreme	Completely secure	1.0 – 0.8
5	High	Guarded, secure area, alarmed	0.8 – 0.6
4	Moderate	Secure area	0.6 – 0.4
3	Low	Complex barriers, security patrols, video surveillance	0.4 – 0.2
2	Very low	Unlocked, non-complex barriers	< 0.2
1	Zero	Completely open, no control, no barriers	0

The load buses are assigned with low security level whereas nuclear power plant's generator buses are considered to have highest security level which corresponds to the extreme level. Similarly, generator buses located at non-nuclear plants are assumed to have high security level and transformer buses enabling energy transfer between separate voltage level grids are regarded as moderate level due to their physical structure. Using normal distribution between each security level a relative degree assignment for each security level is made from 0 to 1.0 as seen in Table.3.

Table 3. Bus Security and Social Criticality Level Distributions

Description	*Security level*	*Social Criticality Degree*	*Physical Reach Degree*
Generator Bus (Nuclear)	Extreme	1.0	0.05
Generator Bus (Non-Nuclear)	High	0.8	0.2
Transformer Bus	Moderate	0.5	0.5
Load Bus	Low	0.2	0.7

Although intentional attack phenomena includes cyber issues, for the test system under study only physical openness is considered as a direct measure of terrorist attack vulnerability. Also, the terrorist attack vulnerability of buses is considered as an indirect measure for line terrorist attack. As the attraction level of bus increased, the relevant line connections to this bus are also expected to increase.

4. Simulation and Analysis

In the scope of this paper, terrorist attack vulnerability evaluation of power transmission lines are made which is the most open part of the transmission system. The proposed vulnerability evaluation is tested using IEEE reliability test system data [11], for which the modified system topology is shown in Fig.3.

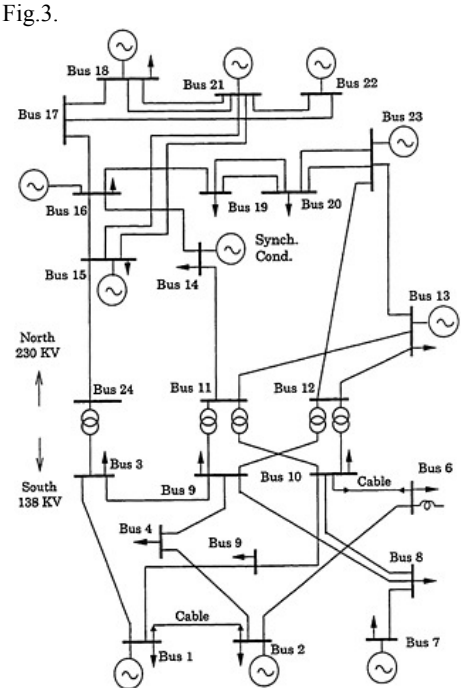

Fig.3. IEEE Reliability Test System Single Line Diagram

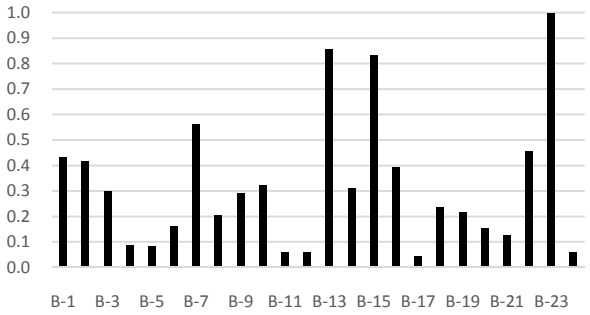

Fig.4. Normalized Terrorist Attack Vulnerability Degree of Buses

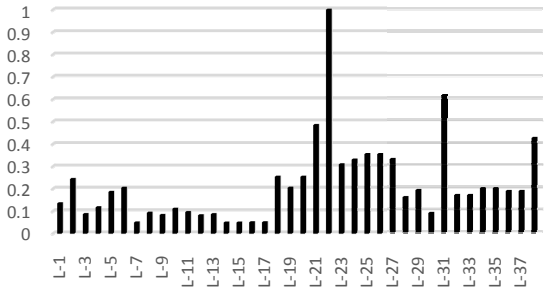

Fig.5. Normalized Terrorist Attack Vulnerability Degree of Lines

For the test system's terrorist attack vulnerability calculation the attraction and accessibility considerations are imposed for buses and lines of IEEE Reliability Test System. The obtained terrorist attack vulnerability rankings for buses and lines are presented in Fig.4 and Fig.5.

According to Fig.4, it is observed that non-nuclear generator buses (B-1, B-2, B-7, B-13, B-15, and B-23) have the highest vulnerability level. However, since the physical attack chance is at lowest level due extreme security, the nuclear power plant generators connected buses (B-18 and B-21) have relatively less level of vulnerability for terrorist acts. Then, transformer buses (B-3, B-9 and B-10) connecting two separate voltage levels have the next higher vulnerability, due their critical role in transfer of energy between different voltage level regions. After terrorist attack vulnerabilities of buses are calculated they are used as an additional parameter in determining indirect vulnerability component evaluation of lines as described in Section-3.

In Fig.5, it should be noted that the longest line, L-31 is not necessarily the most vulnerable line in terms of terrorist attack vulnerability, due to other factors influencing the attraction level. In fact, the lines having same length but located at different voltage levels can have different vulnerability levels due to MVA capacity constraints. Even, the lines, L-10 and L-11, having the same length and installed at the same grid voltage level have different vulnerability ranking. Only, double lines connecting same buses result in same level of attack vulnerability, as expected. So, it is observed that although line length is a direct measure for physical openness, the line capacity and bus criticality are also important parameter for attraction level of sabotage events. The vulnerability evaluation for terrorist attack analysis results are given in Table-4.

Table 4. Analysis Results with Test System Data

From – To	Lines	Length	$V_{TA,l}$
B01 - B02	L-1	3	0.135
B01 - B03	L-2	55	0.244
B01 - B05	L-3	22	0.087
B02 - B04	L-4	33	0.117
B02 - B06	L-5	50	0.186
B03 - B09	L-6	31	0.205
B03 - B24	L-7	0.1	0.049
B04 - B09	L-8	27	0.093
B05 - B10	L-9	23	0.083
B06 - B10	L-10	16	0.111
B07 - B08	L-11	16	0.096
B08 - B09	L-12	43	0.082
B08 - B10	L-13	43	0.086
B09 - B11	L-14	0.1	0.049
B09 - B12	L-15	0.1	0.049
B10 - B11	L-16	0.1	0.050
B10 - B12	L-17	0.1	0.050
B11 - B13	L-18	33	0.254
B11 - B14	L-19	29	0.205
B12 - B13	L-20	33	0.254
B12 - B23	L-21	67	0.485
B13 - B23	L-22	60	1.000
B14 - B16	L-23	27	0.309
B15 - B16	L-24	12	0.330
B15 - B21	L-25	34	0.355
B15 - B21	L-26	34	0.355
B15 - B24	L-27	36	0.332
B16 - B17	L-28	18	0.161
B16 - B19	L-29	16	0.192
B17 - B18	L-30	10	0.090
B17 - B22	L-31	73	0.617
B18 - B21	L-32	18	0.170
B18 - B21	L-33	18	0.170
B19 - B20	L-34	27.5	0.201
B19 - B20	L-35	27.5	0.201
B20 - B23	L-36	15	0.188
B20 - B23	L-37	15	0.188
B21 - B22	L-38	47	0.429

5. Conclusions

In terms of classical electrical system vulnerability evaluation methodology, the electrical features of the system are the main parameters that system's state depends on. However, only considering these parameters may not be enough for a complete vulnerability analysis. Thus, non-operational parameters and other sociological issues that power systems subject to should be included in the vulnerability analysis model. In this study it is shown that, while electrical properties very critical, the priority importance and overall vulnerability degree of the system can change according to the influences from external parameters

such as terrorist attacks. So, with the help of this new knowledge power system operators can update their defense plan's short term activities. Also, TSO's are expected to have further flexibility in limiting cascading failures and alleviating the associated techno-economic impacts. Since analysis of cascading failures is a complicated process and our research is at its early stage, it was not possible to deal with resulting impacts rigorously in this paper. However, we have shown that a broader vulnerability analysis including non-operational factors can assist the system operator in early determination of critical contingencies in order to improve emergency preparedness.

6. References

[1] G. Andersson, P. Donalek, R. Farmer, N. Hatziargyriou, I. Kamwa, P. Kundur, N. Martins, J. Paserba, P. Pourbeik, J. Sanchez-Gasca, R. Schulz, A. Stankovic, C. Taylor, and V. Vittal, (Nov.2005), "Causes of the 2003 Major Grid Blackouts in North America and Europe, and Recommended Means to Improve System Dynamic Performance," IEEE Tran on Power System, Vol. 20, No. 4

[2] M. Marsedek, A.Mohamed, (2012) "Risk based security assessment of power system using generalized regression neural network with feature extraction" http://dx.doi.org/10.1007/s11771-013-1508-9

[3] N. Romero, N.Xu, L.Nozick, I.Dobson, (Feb. 2012) Investment planning for electric power systems under terrorist threat, IEEE Trans. on Power Systems, 27(10): 108–116

[4] J. Salmeron, K.Wood, R. Baldick, (May 2004), Analysis of Electric Grid security under terrorist threat, IEEE Transactions Power Systems 19 (2) (2004) 905-912

[5] A. Delgadillo, J.M. Arroyo, N. Alguacil, Analysis of Electric Grid Interdiction with Line Switching, IEEE Transactions on Power Systems

[6] G. Brown, M. Carlyle, J. Salmeron, K. Wood, Analyzing the vulnerability of critical infrastructure to attack and planning defenses, INFORM 2005, doi:10.1287/educ.1053.0018

[7] E. Zio, R. Piccinelli, G. Sansavini, (2012), "A Framework for Ranking the Attack Susceptibility of Components of Critical Infrastructures," Chemical Engineering Transactions Vol. 26

[8] IEEE C2: National Electrical Safety Code, C2-1997

[9] E.Zio, R.Piccinelli and G.Sansavini, (2011), "An All-Hazard Approach for the Vulnerability Analysis of Critical Infrastructures," ESREL, Troyes

[10] Y.Li, S. Chu, (2014) "Construction and Reduction Methods of Vulnerability Index System in Power SCADA," International Journal of Security and Its Applications, Vol.8, No.6

[11] The IEEE reliability test system: 1996, Grigg, C., Paper 96 WM 326-9 PWRS, IEEE Winter power meeting 1996