Vulnerability Indices For Power Systems

Mingoo Kim, *Member, IEEE*, Mohamed A. El-Sharkawi, *Fellow, IEEE*, and Robert J. Marks II, *Fellow, IEEE*

***Abstract*-- The purpose of vulnerability assessment is to determine when a disruption of service is likely to occur and to take steps to reduce the associated risk. With the growth of power systems, increases in grid complexity, and the trend toward deregulation, vulnerability assessment is imperative. Accurate vulnerability assessment is especially vital during heavy loading conditions and a vulnerability index is greatly needed to help the operator steer the system to viable conditions. In this paper, two new vulnerability assessment methods are proposed. One is based on the distance of the current operating point from the vulnerability border of the system. The other is an index based on the anticipated loss of load. These two methods are fully applicable to the case of cascading events.**

***Index Terms* -- Particle swarm optimization, security assessment, vulnerability assessment, vulnerability index.**

I. Introduction

THE purpose of vulnerability assessment is to determine a power system's ability to continue to provide service in case of an unforeseen catastrophic contingency. A power system can become vulnerable for various reasons, including component failures, communication-system failures, human operator errors, weather conditions, and human errors.

An approach to power system vulnerability assessment begins with the analysis of system behavior for credible system contingencies. If analysis indicates that the system is vulnerable, preventive strategies should be implemented to steer the system to a more viable operating point, thus forestalling the possibility of cascading outages. A power system is invulnerable if it can withstand all credible contingencies without violating any of the system constraints. If there is at least one contingency which violates the system constraints, the system is judged to be vulnerable.

The purpose of a vulnerability index is to reflect the level of system strength or weakness relative to the occurrence of an undesired event. The vulnerability of a power system increases when the operating conditions change so as to increase the likelihood of a blackout.

When a system is to be judged vulnerable /invulnerable, quantitative measures to assess the degree of vulnerability/invulnerability are needed. The most common vulnerability/security indexes are the c*ritical clearing time* (CCT) and the *energy margin* (EM). The CCT is the maximum elapsed time from the initiation of a fault until the fault is isolated and the power system remains transiently stable [1,2]. This intensive approach, however, is computationally prohibitive, thereby limiting its usefulness to limited number of off-line studies.

To overcome this weakness, direct methods have been developed [3-7]. In contrast to the time-domain approach, the direct method determines system stability from energy functions by comparing the energy levels of the system to a pre-selected critical energy value. The difference is known as the *energy margin* (EM) and can be used as a vulnerability/security index. Direct methods have a long history of development [3-7], but, until recently, many researchers have thought of them as impracticable for detailed large-scale power system analysis because of intrinsic modeling limitations. Moreover, direct methods are less accurate than the time domain approach [7].

Knowledge of the vulnerability border can provide an operator with valuable guidance for steering the power system away from vulnerable operating regions. Moreover, the identification of the vulnerability border can provide easily understood visual information to the operator. The distance of the current operating point from the border provides a direct assessment of the degree of vulnerability, which is, in itself, a vulnerability index. The vulnerability boundary, however, cannot be determined analytically for a large-scale power system, requiring, rather, extensive computation by numerical methods.

Most utility companies in North America use *nomograms* to characterize the security boundaries [8]. Fig. 1 is an example of a typical nomogram showing three levels of the security indices (SI).

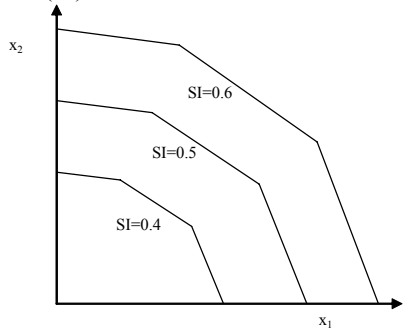

Fig. 1. Nomogram for two parameters showing three security levels.

In developing a nomogram, two critical parameters are chosen, denoted, respectively, by x_1 and x_2 in Fig. 1. All other critical parameters are then set to default values. Points on the nomogram curve are plotted by repeated computer simulations.

Mingoo Kim is with Samsung, Korea.

Mohamed A. El-Sharkawi is with the university of Washington, Seattle, WA 98195 (e-mail: elsharkawi@ee.washington.edu).

Robert J. Marks is with Baylor University, Waco, Texas 76798 (e-mail: Robert_Marks@baylor.edu).

1-59975-028-7/05/$20.00 © 2005 ISAP.

Because this process requires intensive computer simulation, usually only a few points on the boundary, *corner point*, are calculated. The remaining segments of the curves are obtained using linear interpolations. This approximation can result in significant inaccuracies due to the limited number of critical parameters [8].

In order to overcome these drawbacks, security-border identification algorithm using *neural network* (NN) inversion was proposed [9,10]. The NN was trained to predict the security ranking, and the security border could be effectively identified by NN inversion. Due to the quick response of the NN as a power-system emulator, the process of border identification can be done quickly. Moreover, there is no limitation on the number of critical parameters for the simulations. In [11], an enhanced *particle swarm optimization* (PSO) search algorithm was applied to NN inversion to identify the vulnerability border faster than previously possible. More importantly, the border can be dynamically updated to reflect changes in power-system topology.

In this paper, two new vulnerability indices are proposed. The first is based on the distance from the vulnerability border, and the other is based on the anticipated loss of load.

II. Vulnerability Index Based on Distance from Border

The proposed *vulnerability index* (VI) in this section is based on the distance of a given operating point from the border of vulnerability. The method allows straightforward visualization. Simultaneous display of the current operating state and the closest vulnerability border point enables the operator to see important information at a glance.

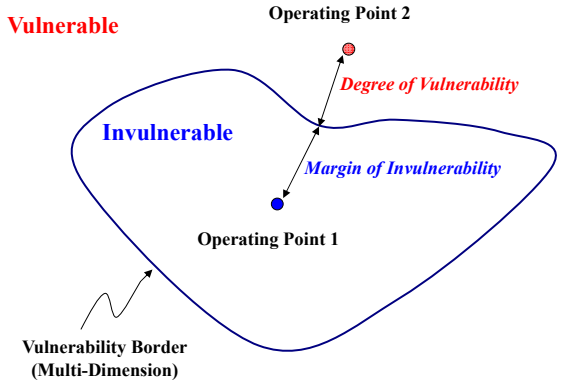

Fig. 2. Vulnerability border.

Consider the schematic representation of the operating space of the power system in Fig. 2. If a given operating point lies inside the border, the operating state of the system is said to be invulnerable and the distance from the closest point of the border would be the margin of safety. On the other hand, if an operating point lies outside the border, the operating state is said to be vulnerable and the shortest distance to the border is the degree of vulnerability. By this approach, the vulnerability index computed on the output space (CCT, energy margin, etc.) can explicitly reflect the information on the input space (voltages, currents, powers, etc.).

The proposed algorithm starts by training the neural network off-line to predict the vulnerability status of a power system with the 24-hours load profiles. The NN module provides a VI in the output space. This process can be modeled by mapping $VI = f_{NN}(\vec{x})$, where $\vec{x}$ comprises the power system features chosen to represent the operating state, VI is the vulnerability index, and $f_{NN}(\ )$ is the neural network model. The output of the neural network module is the vulnerability index or any other possible index such as the Critical Clearing Time (CCT) or the Energy Margin (EM). The desired VI of the border is set by the operator. The PSO algorithm [11] seeks to find the closest border point by minimizing an objective function F, of the following form:

$$F = \left| f_{NN}(\vec{x}) - VI_{desired} \right| + w \times \left\| \vec{x} - \vec{x}_{Operating} \right\|,$$

where

f_{NN} is the neural network function,

$\vec{x}$ is the current position of a given particle,

$\vec{x}_{Operating}$ is the position of the operating point,

$\| \ \|$ is the Euclidean distance between $\vec{x}$ and $\vec{x}_{Operating}$

w is a weighting factor.

The function of the PSO is to find the border points as well as the minimum distance from the operating point [11].

A. Particle Swarm Optimization(PSO)

The PSO algorithm is one of the evolutionary techniques developed by Eberhart and Kennedy [12, 13]. PSO is a powerful multi-agent search technique modeled on movement of bird flocks in flight. Each individual (agent or bird) is dubbed a "particle" and represents a potential solution. Each particle adjusts its path according to its own experience and that of its companions. Through cooperation and competition among potential solutions, this technique can often find optima relatively quickly in complex optimization problems.

The basic PSO concept consists of changing the velocity and the position of each particle incrementally along a time axis. Its movement is expressed by Equations (1) and (2):

$$\vec{v}(k+1) = w \times \vec{v}(k) + c_1 \times rand() \times (\vec{x}_{SelfBest}(k) - \vec{x}(k)) + c_2 \times rand() \times (\vec{x}_{GroupBest}(k) - \vec{x}(k)) \quad (1)$$

$$\vec{x}(k+1) = \vec{x}(k) + \vec{v}(k) \quad (2)$$

$\vec{x}$ is the solution vector of a single particle and $\vec{v}$ is the velocity. Equation (1) is used to calculate the new velocity of each particle and Equation (2) is used to ascertain its position. The acceleration constants c_1 and c_2 represent the weighting of the stochastic acceleration term. Experiences with PSO have shown that, for most applications, these design parameters work best when both are set to 2.0 [12, 13].

In Equation (1), *rand( )* represents a uniform random number between *0* and *1*. The two random numbers in Equation (1) are independently generated.

GroupBest is the best point found among all the particles in the group, which is tantamount to best experience of the particles as a group. *SelfBest* is the best point observed by the current particle, representing its own best experience.

B. Case Study

The proposed method is tested using the WSCC (Western Systems Coordinating Council) 179-bus system. The WSCC 179-bus test system has 29 generators, 203 transmission lines, and 179 buses. This system is an equivalent representation of the interconnections in the western United States.

The data set for a cascading event was generated. One of the three parallel 500kV transmission lines between John Day and Grizzly substations was used as a trigger for the events. Fig. 3 shows a zoomed section of the system where the events occurred.

The first event was assumed to be a three-phase fault at one of the triple lines between bus #82 and bus #76. After 10 ms, one of the parallel lines between bus #76 and bus #78 was opened, simulating a second event. Finally, one of the parallel lines between bus #78 and bus #80 was opened 10 ms after the second event. For each of these events, the CCT was used as a vulnerability index. Any other measure for vulnerability could be used. In order to vary the operating conditions, all generator outputs and loads were randomly changed between 70%- 140 %.

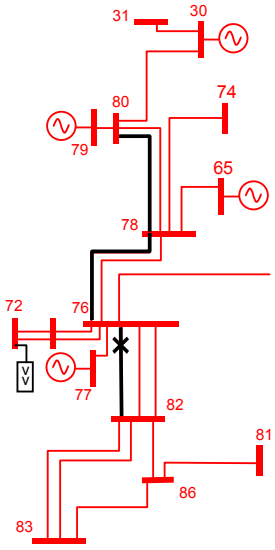

Fig. 3. One-line diagram of the studied section.

A total of 1000 possible operating points were used. Figs. 4, 5, and 6 present the histogram of the error in the CCT after each event. The CCT error is the difference between the CCT of the border point as computed by the model, and that of the point subsequently found by the PSO. This can be taken as a measure of the accuracy of the PSO algorithm in finding border points. As seen in these figures, the PSO is very effective in finding the border points.

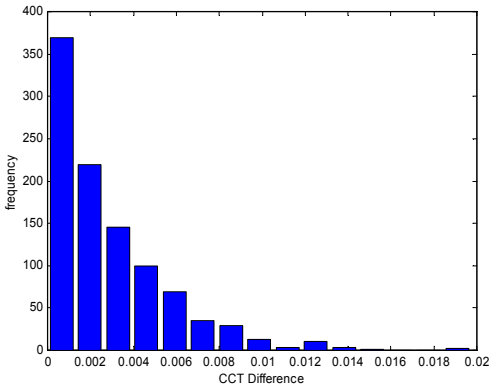

Fig. 4. Distribution of CCT error after the first event.

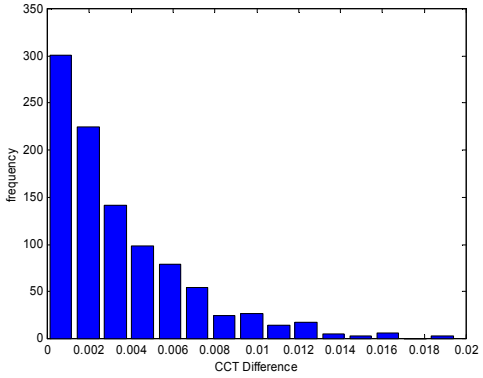

Fig. 5. Distribution of CCT error after the second event.

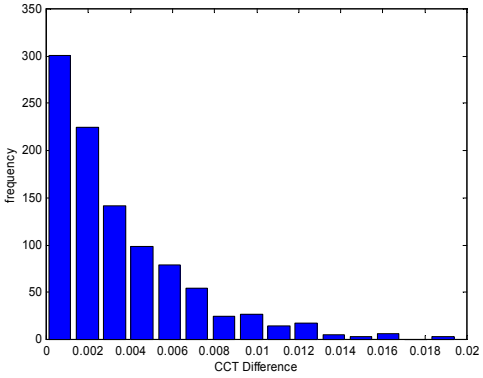

Fig. 6. Distribution of CCT error after the third event.

C. Visualization of System Vulnerability

A visualization tool can be developed to provide the operator with an illustration of system vulnerability. To have an effective illustration, the visualization is developed for the input space, where the variables are explicit (voltages, powers, etc.). The VI, in this case, is the Euclidean distance between the current operating point and the nearest border point as described by the explicit variables.

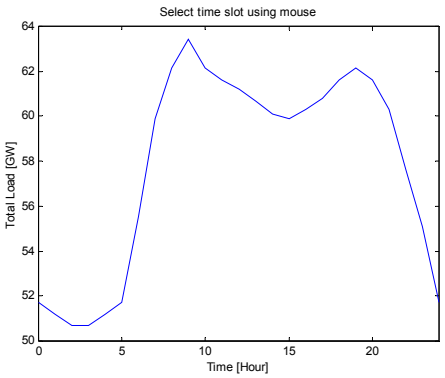

Fig. 7. Arbitrarily selected load curve.

For the test system and fault scenarios described above, the system load is assumed to be the 24-hr load curve shown in Fig. 7. The system is described by 30 variables of real and reactive powers. These variables are chosen by using a feature extraction technique [14]. An operating point is a single vector that includes all the 30 variables.

Figs. 8 and 9 show the visualization of the system vulnerability at 10 a.m. when the system demand is about 62 GW as shown in Fig. 7. The superimposed bars in the figures represent the magnitude of the variables in the operating space (dark shading), and the value of the variables at the nearest feasible border point (light shading). The vulnerability index as defined by the Euclidean distance is also shown at the far right in the figures. A negative vulnerability index represents an invulnerable operation. Its magnitude is the vulnerability margin. A positive magnitude represents a vulnerable operation, and its magnitude is an indication for the degree of system vulnerability. As seen in Fig. 8, all variables are less or equal to these at the nearest border point. This is invulnerable operation and the vulnerability index is about 20%.

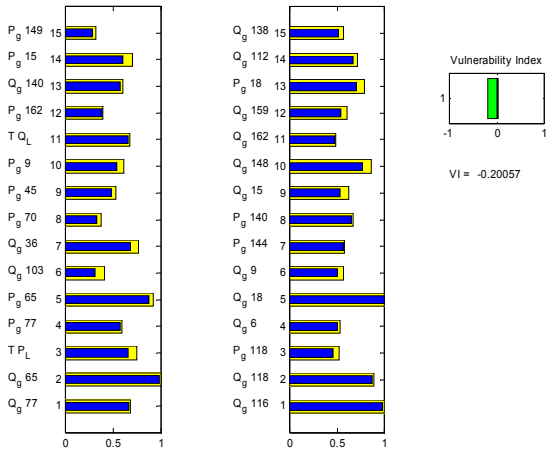

Fig. 8. Current operating points and border after the first event.

After the second event, the system vulnerability is shown in Fig. 9. As seen in the figure, most variables clearly exceed the border point, and the system is vulnerable. The vulnerability index is positive and its numerical value (50%) indicates how far the system is from the border.

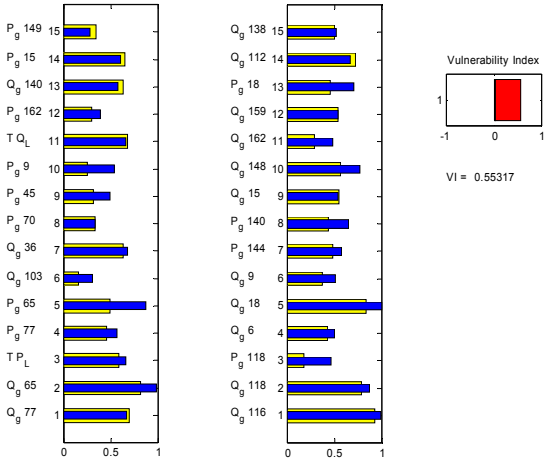

Fig. 9. Current operating points and border after the second event.

The above visualization can be performed on-line. The execution time is in milliseconds on Pentium PCs.

III. Vulnerability Index Based on Anticipated Loss of Load

In section II, a vulnerability index based on the distance from a defined border is proposed. This border can be ascertained on the basis of any one of a number of different indices. In the previous section, however, the CCT was used for this purpose.

Since the purpose of vulnerability assessments is to allow avoidance of catastrophic power outages in the case of cascaded events, the index should reflect how much load might be lost at such times. Hence, we are proposing to use the anticipated loss of load as an alterative index. This concept is simple but requires a great deal of off-line computation. In the case of small systems, one can examine all possible combinations of load reductions to find an appropriate minimum. However, for systems of the size normally encountered, an exhaustive search is impracticable. Suppose that we shed each load from 0% to 100% in increments of 1%. If a system has N loads, there are 100^N possible combinations of load reductions. Such a number is well beyond the limits of current computation. To address this issue, we propose using PSO to find the best possible combination of load reductions while maintaining stability. This is a sub-optimal process. The amount of load shed in this case is the vulnerability index.

A. Under Frequency Load shedding

Normally, power systems are operated under quasi-equilibrium conditions where the total load consumption and system losses equal the total generation. System frequency is governed by this equilibrium and consequently, any unbalance in loads can result in frequency excursions that may lead to loss of synchronism. An excess of load results in a system frequency drop and load shedding has to be employed in order to rapidly balance demand and generation.

Load shedding is accomplished using frequency sensitive relays that detect the onset of decay in power system

frequency where both frequency and rate of frequency decline are measured. Load shedding is usually implemented in stages each of which is triggered at a different frequency level or at specified rate of frequency decline [15-17].

In [18], a load shedding scheme is developed based on frequency decline and on the rate of frequency decline. Table 1 shows the step size and time delay for a typical scenario. The notation "C" represents the time delay in cycle. A more detailed explanation of Table I is provided in [18]. This scheme is used for comparison of the procedure we propose.

TABLE I
STEP SIZE AND DELAY TIME OF THE TWO LAYERS AS PERCENTAGE OF THE TOTAL LOAD

	59.5 Hz	59.3 Hz	58.8 Hz	58.6 Hz	58.3 Hz
Activated by frequency decline rate	20 % (0C)		5 % (6C)	4 % (12C)	4 % (18C)
Activated by frequency decline		10 % (28C)	15 % (18C)		

B. Optimal Load Shedding by Particle Swarm Optimization

Load shedding is a combinatorial optimization problem that lends itself to the particle swarm optimization (PSO) technique. The overall procedure of this method is shown in Fig. 10. The starting point of this procedure is to determine the dimension of the search space. We can search all possible combination of load reduction, but it may lead to unacceptable computational time. Extended Transient-Midterm Stability Program (ETMSP) is used in this analysis. However, since ETMSP doesn't monitor the frequency of load buses, under frequency load shedding relays are installed at all load buses to detect which loads are to be shed due to the frequency decline.

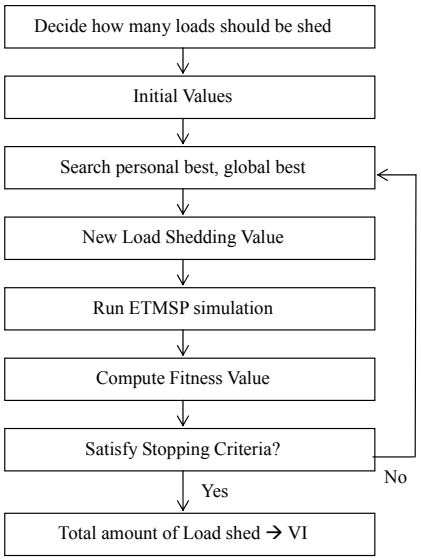

Fig. 10. The overall procedure of PSO method.

After determining the buses for load shedding, each PSO agent (particle) traverses the search space looking for the global minimum combination of load shedding using the initial values obtained in the previous step. These best points are verified using ETMSP simulation.

Equations (3) and (4) show the fitness values that PSO is to maximize. It is the inverse of the summation of all load reductions. This fitness function will have a maximum value when all loads are maintained. If the system is unstable, the fitness function has a negative sign.

$$F = \frac{1}{\sum MVA}, \quad \text{if system is stable} \tag{3}$$

$$F = -\frac{1}{\sum MVA}, \quad \text{if system is unstable} \tag{4}$$

After each iteration, the fitness value of the global best point is compared with the fitness at the previous iteration. If the difference is smaller than a set value, and is maintained small for several iterations, a solution is achieved and the amount of load shedding is the vulnerability index.

C. Test Scenario 1

The scenario used in test case 1 is a sequence of events that leads to simultaneous loss of the lines between the following buses.

Bus 83 - Bus 172
Bus 83 - Bus 168
Bus 83 - Bus 170

To save the system from an impending blackout, the system was split into two island 0.2 seconds after the contingency. In order to create the islands, the following lines are opened:

Bus 133-Bus 108
Bus 133-Bus 104
Bus 29 - Bus 14

This scenario was used in [18].

The ETMSP is used to simulate the system assuming the load buses are equipped with under frequency relays. The relay settings are shown in Table I. To stabilize the system, a total of nine loads were shed. The PSO method was also used to search for the minimum amount of load shedding. The PSO technique searched among the same load buses identified by the under frequency relay method.

The results of both methods are shown in Fig. 11. The x-axis shows the bus numbers and the y-axis represents the amount of load shed by each method. The unit of y-axis is MVA. As seen in the figure, the PSO method achieves a smaller amount of load shedding as compared with the under frequency relay method. The total system load shed by the PSO method is less than 60 % of that computed by the under frequency relay method.

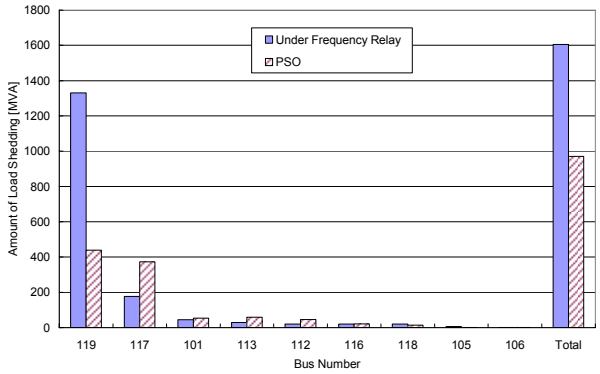

Fig. 11. The amount of load shedding.

D. *Test Scenario 2*

A second example is used to test the proposed technique. In this example, a three phase permanent fault on line 83-86 near bus 83 is assumed as shown in Fig. 12.

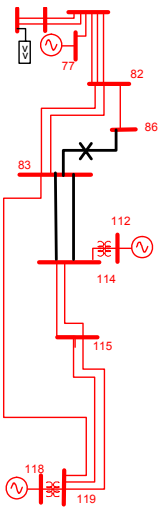

Fig. 12. One-line diagram of the studied section.

Allowing for the breakers actuation delays and normal relay actions, the line was cleared within 50 ms. One type of hidden failure identified in the literature [19] occurs in transfer trip systems involving directional-comparison blocking. If such a system were employed here, the relays in the unfaulted parallel 83-114 lines would see the fault but would be inhibited from tripping by the blocking signal. The loss of both of these lines results in an unstable condition and under frequency relay couldn't stabilize the system. However with PSO, we can find a combination of load shedding that would render the system stable. Under these conditions, it was found that shedding a system load of only 98 MVA would stabilize the system.

E. *Example of Vulnerability Index Based on Anticipated Loss of Load*

Test cases show the feasibility of the proposed technique. The anticipated loss of load, as obtained by the PSO technique, can be used as a vulnerability index. This index is applicable in the case of cascading events. Moreover, any control actions can be considered in the course of the relevant calculations.

Fig. 13 is a histogram for the minimum amount of load shedding for Test Scenarios 2. The figure shows the frequency distribution of the total magnitude of load shedding for different loading configurations. In this test, 1500 different operating conditions were considered.

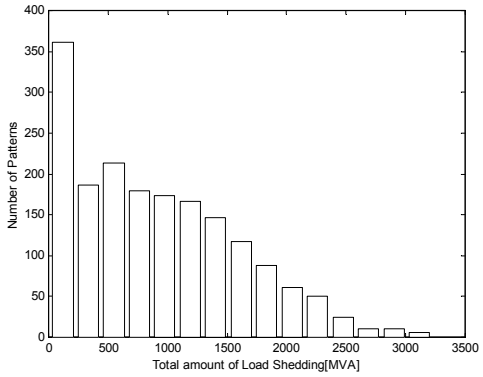

Fig. 13. Distribution of the total magnitude of load shedding.

The amount of load shedding in MVA can be used directly as a VI, which provides the operator with a measure that can be immediately understood. This amount could be normalized between 0 and 1. Another choice is to take the percentage with respect to the total load demand. In this example, the highest load shedding required is 3.15 GVA. The corresponding load demand is 68.4 GVA. The load shedding percentage (4.6 %) can be taken as an alternative expression for the vulnerability index VI.

IV. Conclusion

In this paper, we propose two new vulnerability indices. The first is a vulnerability index based on distance from the vulnerability border as identified by Particle Swarm Optimization. This procedure is highly amenable as a visualization tool. Simultaneous display of the current operating state and the closest vulnerability border point enables the operator to see important information at a glance. The other is an index based on anticipated loss of load. This index is fully applicable in the case of cascading events. Moreover, any relevant control actions can be incorporated into the ongoing calculations. The PSO algorithm was used to handle the extensive computation required for finding the best combination of load reductions. Test results show this technique can ascertain the minimum amount of load shedding required within a reasonable time.

V. Acknowledgements

The authors would like to acknowledge the National Science Foundation, the Electric Power Research Institute and the Advanced Power Technology Laboratory at the University of Washington for their financial support of this research.

VI. REFERENCES

[1] P. Kundar, Power System Stability and Control, McGraw-Hill, 1994.

[2] M. Moechtar, T. C. Cheng, and L. Hiu, "Transient Stability of Power System – A Survey," WESCON '95, 1995, pp.166-171.

[3] P. C. Magnusson, "The Transient-Energy Method of Calculating Stability," Trans. AIEE, vol.66, 1947, pp.747-755.

[4] G. E. Gless, "Direct Method of Lyapunov Applied to Transient Power System Stability," IEEE Trans. Power Apparatus and Systems, vol.PAS-85, 1966, pp.159-168.

[5] T. Athay, R. Podmore, and S. Virmani, "A Practical Method for the Direct Analysis of Transient Stability", IEEE Transactions on Power Apparatus and Systems, Vol. PAS-98, No. 2, March/April 1979, pp. 573-584.

[6] A. A. Fouad and V. Vittal, Power System Transient Stability Analysis Using the Transient Energy Function Method, Prentice Hall, 1992.

[7] H. Chiang, C. Chu, and G. Cauley, "Direct Stability Analysis of Electric Power Systems Using Energy Functions: Theory, Applications, and Perspective", Proceedings of the IEEE, November 1995, pp.1497-1529.

[8] J. McCalley et al, "Security Boundary Visualization for Systems Operation," IEEE Trans. On Power Systems, Vol.12, May 1997, pp.940-947.

[9] C. A. Jensen, M. A. El-Sharkawi, and R. J. Marks, "Location of Operating Points on the Dynamic Security Border using Constrained neural Network Inversion," *Proc. Int. Conf. Intelligent Systems Applications to Power Systems (ISAP '97)* , Seoul, Korea, 1997.

[10] C. A. Jensen, R. D. Reed, R. J Marks, M. A. El-Sharkawi, Jae-Byung Jung, R. T. Miyamoto, G. M. Anderson, and C. J. Eggen, "Inversion of feed-forward neural networks: Algorithms and applications", Proceedings of the IEEE , Volume: 87 Issue: 9 , Sept. 1999 Page(s): 1536 -1549.

[11] Ioannis N. Kassabalidis, M. A. El-Sharkawi, R. J. Marks II, Luciano S. Moulin, and A. P. Alves da Silva, "Dynamic Security Border Identification Using Enhanced Particle Swarm Optimization," IEEE Transactions on Power Systems, pp. 723-729, August 2002.

[12] J. Kennedy and R. Eberhart, "Particle Swarm Optimization," Proc. IEEE Int'l. Conf. on Neural Networks, Piscataway, NJ: IEEE Press, pp.1942–1948, 1995.

[13] R. Eberhart and J. Kennedy, "A New Optimizer Using Particle Swarm Theory," Proceedings of the Sixth International Symposium on Micro Machine and Human Science, Nagoya, Japan, Piscataway, NJ: IEEE Press, pp.39-43, 1995.

[14] C. A. Jensen, M. El-Sharkawi and R. J. Marks, "Power System Security Assessment Using Neural Networks: Feature Selection Using Fisher Discrimination", IEEE Transactions on Power Systems, pp. 757-763, November 2001.

[15] S. Grewal, J. Konowalec, and M. Hakim, "Optimization of a load shedding scheme, " IEEE Industry Applications Magazine , Vol.4 , July-Aug. 1998 pp. 25 -30.

[16] R. Anderson, *Power System Protection*, IEEE Press, 1999.

[17] S. Lindahl, G. Runvik, and G. Stranne, "Operational Experience of Load Shedding and New Requirements on Frequency Relays," *Developments in Power System Protection*, March 1997, pp. 262-265.

[18] J. McCalley and V. Vittal, "On-Line Risk-Based Security Assessment," Final Report, EPRI WO663101, November 2000.

[19] A. G. Phadke, S. H. Horowitz, and J. S. Thorp, "Anatomy of power system blackouts and preventive strategies by rational supervision and control of protection systems," ORNL Report, ORNL/Sub/89-SD630C/1, Jan. 1995.

VII. BIOGRAPHIES

Mingoo Kim received his BS and MS degrees in 1994 and 1996, respectively, from Kwangwoon University in Seoul. His areas of interest include power systems and computational intelligence. In 2002 he earned a Doctor of Philosophy at the University of Washington in Electrical Engineering.

Mohamed A. El-Sharkawi is a Fellow of the IEEE. He received his B.Sc. in Electrical Engineering in 1971 from Cairo High Institute of Technology, Egypt. His Ph.D. in Electrical Engineering was received from the University of British Columbia in 1980. In 1980 he joined the University of Washington as a faculty member where he is currently a Professor of Electrical Engineering. He is the vice president of the IEEE neural networks society. He is the founder and co-founder of several International Conferences including the *Application of Neural Networks to Power Systems (ANNPS)*, and *Intelligent Systems Applications to Power (ISAP).* He is the co-editor of several IEEE tutorial books on the applications of *intelligent systems to power systems.* He has published over 160 papers and book chapters. He holds five patents.

Robert J. Marks, II (Fellow, IEEE) is a Professor and Graduate Program Coordinator in the Department of Electrical Engineering, College of Engineering, University of Washington, Seattle. He is the author of numerous papers and is coauthor of the book *Neural Smithing: Supervised Learning in Feedforward Artificial Neural Networks* (MIT Press, 1999). Dr. Marks is a Fellow of the Optical Society of America. He served as the first President of the IEEE Neural Networks Council. In 1992 he was given the honorary title of Charter President. He served as the Editor-in-Chief of the IEEE TRANSACTIONS ON NEURAL NETWORKS and as a Topical Editor for Optical Signal Processing and Image Science for the *Journal of the Optical Society on America* A.
For more information see: cialab.ee.washington.edu/Marks.html.