New Monitoring and Control Scheme for Preventing Cascading Outage

Nan Zhang, *Student Member, IEEE,* Hongbiao Song, *Student Member, IEEE,*
and Mladen Kezunovic, *Fellow, IEEE*

***Abstract*—This paper presents a new approach for preventing cascading outage by coordinated system and local monitoring and control scheme. System monitoring evaluates the vulnerability and security of the power system during dynamic changing conditions. It finds the vulnerable power system components indicating that their protective relays need to be monitored closely. Local monitoring can provide the exact disturbance information and monitor the correctness of the actual relay operations. If the relays act improperly, the proposed approach enables one to mitigate the disturbance or prevent the possible cascading outage. Further system control actions may be chosen based on the local information update. Several examples using the IEEE test system demonstrate the advantages of this approach.**

***Keywords*—Cascading outage, control, event tree analysis, fault analysis, fault location, monitoring, neural networks, power system stability, relaying, security analysis, system-wide disturbance.**

I. Introduction

Power system cascading outage is quite often a complicated phenomenon, which may finally result in a large area blackout. There are many factors contributing to power system cascading outages, such as inadequate understanding of unfolding events, inadequate operational awareness, inadequate tree trimming, relaying problems, bad weather conditions, human errors, etc [1]. No single factor may be the cause of system cascading outage and large area blackout. From the technical side, relaying problems and inadequate understanding of unfolding events are two major contributing factors, although neither of them may be the triggering cause. Relaying problems were the contributing factor in almost 70% of the US disturbances from 1984 to 1991 [2]. Relay failure and misoperation during weakened system conditions contribute the most to the cascading outages. Another problem is that power system operators lack sufficient analysis and decision support to take quick corrective actions due to inadequate understanding of unfolding events. This was clearly demonstrated in the August 1996 US Western Coast System Blackout and August 2003 US Northeastern System Blackout [1,3].

Different research efforts are aimed at understanding and finding ways to prevent cascading outages: dynamical and probabilistic study of the cascade model, dynamic decision-event tree analysis, wide area back-up protection expert system, relay hidden failure analysis, special protection scheme, etc [4-7]. However, there are no effective interactive monitoring and control tools developed so far to detect and mitigate the cascading outage. This paper introduces a new interactive scheme of system/local monitoring and control tools for efficiently dealing with cascading outages.

II. Basic Idea of the New Scheme

The proposed system monitoring and control tool is intended for installation at the control center. It consists of routine and event-based security analyses. For the routine static and dynamic contingency analysis, contingencies which can lead to an overload condition, voltage problem, angle stability, voltage stability, etc., will be found and taken care of. Either preventive control actions need to be taken to prevent such problems or emergency control needs to be activated if such contingencies have really happened. Vulnerability analysis of operating condition of the whole system and individual element can be implemented as discussed in this paper. Vulnerable elements will be located and their relays need to be closely monitored. The event-based security analysis is triggered when a disturbance occurs. It will indicate whether the emergency control is needed to mitigate the transient stability problem or not.

The local monitoring and control tool is intended for installation at local substations. Neural network based fault detection and classification, synchronized sampling based fault location, and event tree analysis can be combined as an advanced real time fault analysis tool and relay monitoring system as described in this paper. This will provide detailed information about disturbance and relay operations for each related local substation.

The online implementation of the system as well as local monitoring and control tools proposed in this paper will follow these steps:

Step 1: Routine vulnerability and security analysis performed by the system tool: (a) decides security level and finds vulnerable elements, then sends monitoring command to the local tool; (b) identifies critical contingencies, and starts associated control schemes to find the control means for those expected events.

This work is supported by NSF I/UCRC called Power Systems Engineering Research Center (PSerc), project titled “Detection, Prevention and Mitigation of Cascading Events”, and in part by Texas A&M University.

N. Zhang, H. Song and M. Kezunovic are with the Department of Electrical Engineering, Texas A&M University, College Station, TX 77843-3128, USA (e-mails: zhangnan@ee.tamu.edu, songjefferson@tamu.edu, kezunov@ee.tamu.edu)

0-7803-9255-8/05/$20.00 2005 IEEE

Step 2: Local monitoring performed by the local tool: (a) starts analysis when disturbance occurs; (b) if it finds relay misoperation, it makes correction or receives system control command for better control; (c) reports disturbance information and analysis to the system tool.

Step 3: Event-based security analysis performed by the system tool: (a) if it finds a match with expected event, activates the emergency control; (b) if it does not find a match, analyzes if the system is secure or not; (c) if it is not, finds new emergency control and activates it.

Step 4: Update information and go to Step 1.

III. System monitoring and control tool

A. Vulnerability Analysis

Vulnerability Index (*VI*) method is a good way to assess the vulnerability of individual elements and the entire system in steady state. Vulnerability Indices of the generation part, bus part and transmission part can be easily calculated based on results of power flow method or fast approximate method. The detailed description of this method can be found in [8]. Here we only give the final equations of Vulnerability Indices for generation part, bus part, transmission part and the whole system as follows:

$$VI_{gen} = \sum_{i=1}^{m} (VI_{Pg,i} + VI_{Qg,i} + VI_{gen\_loss,i}) \tag{1}$$

$$VI_{bus} = \sum_{i=1}^{n} (VI_{V,i} + VI_{Loadab,i} + VI_{load\_loss,i}) \tag{2}$$

$$\begin{aligned} VI_{line} = \sum_{i=1}^{p} (VI_{Pf,i} + VI_{Qf,i} + VI_{Qc,i} \\ + VI_{line\_ang,i} + VI_{\mathrm{Re}lay,i} + VI_{line\_off,i}) \end{aligned} \tag{3}$$

$$VI = W_{gen} VI_{gen} + W_{bus} VI_{bus} + W_{line} VI_{line} \tag{4}$$

where

-VI_{gen}, VI_{bus}, VI_{line}, VI: Vulnerability Indices for all generators, buses and transmission lines and the whole system

-W_{gen}, W_{bus}, W_{line}: Weights for generation part, bus part and transmission part

By this method, we can evaluate system vulnerability information about different conditions and find individual elements that are most vulnerable.

B. Static Contingency Analysis

For a small system, one or two line outages may lead to system islanding. Even for a large system, different control areas may have limited number of tie-lines. If they are disconnected, the whole system may split into several smaller systems and cascading outages may occur in those smaller systems if they are unbalanced. Thus, some critical lines must be identified. The relays at these lines need to be monitored. If they misoperate, system security may be decreased. We use the topology processing method based on the node-branch incidence matrix to find the single transmission line list (for N-1 contingency) and critical line pair list (for N-2 contingency).

The fast Network Contribution Factor (NCF) method is used to do the N-1 and N-2 static contingency analysis. It calculates the line flow change and bus voltage change with satisfactory accuracy based on the base load flow condition and network information. Detailed description can be found in [8]. For the most vulnerable contingencies, full AC power flow should be run to verify the final results.

C. Dynamic Contingency Analysis

Transient stability analysis and voltage stability analysis need to be implemented to check whether there is an angle stability or voltage stability problem. If the critical clearing time (CCT) is smaller than the backup tripping time for specific disturbance on specific line, the relay at this line needs to be monitored and associated emergency control needs to be defined for such contingency.

The relay operation can also be simulated during dynamic contingency analysis. From the time-domain transient stability program, the phasors of generator bus voltages and current injections can be obtained using certain transformation. We can calculate the bus voltage phasor information in order to get the rough dynamic apparent impedance seen by distance relay. Here we give a simple description [9].

$$\begin{bmatrix} I_g \\ I_l \end{bmatrix} = \begin{bmatrix} Y_{gg} & Y_{gl} \\ Y_{\mathrm{lg}} & Y_{ll} \end{bmatrix} \begin{bmatrix} V_g \\ V_l \end{bmatrix} \tag{5}$$

Assuming constant impedance load model, that is, $I_l = 0$, we can get

$$V_l = -(Y_{ll})^{-1} Y_{\mathrm{lg}} V_g \tag{6}$$

Apparent impedance seen by distance relay

$$\bar{z}_{ij} = \frac{V_i}{I_{ij}} = \frac{V_i}{V_i - V_j} z_{ij} = d_{ij} z_{ij} \tag{7}$$

where z_{ij} is the impedance of line i-j.

For the line distance relay (with mho characteristic), it will operate if

$$\left| \bar{z}_{ij} - \rho \right| \le \left| \rho \right| \tag{8}$$

where $\rho = \beta z_{ij} / 2$

Normalize as $\left| d_{ij} - \beta / 2 \right| \le \beta / 2$

(9)

By this method, we can check whether the dynamic apparent impedance falls into the distance relay protection zones or not. For example, it may appear that the system is stable because of fault clearing time smaller than CCT from the transient stability viewpoint, while distance relay sees apparent impedance falling into its protection zone so it may trip the line. Cascading outage may occur.

D. Steady State Control Scheme

The comprehensive congestion management control scheme was proposed in [10] based on the Network

Contribution Factor (NCF) method, Generator Contribution Factor (GCF) method and Load Contribution Factor (LCF) method. It can solve the steady state problems, such as overload, low/high voltage, line-flow re-dispatching, etc.

E. Transient Stability Control Scheme

The transient stability control scheme was proposed in [11] based on the Potential Energy Boundary Surface (PEBS) method and analytical sensitivity of the transient energy margin. This method may be used to find the most contributing control method to stabilize the system and its final results can be verified using the time domain transient stability program.

IV. Local monitoring and control tool

To improve the real-time fault analysis of conventional distance relays, an advanced fault analysis tool combined with the neural network based fault detection and classification (NNFDC) and synchronized sampling based fault location (SSFL) is proposed. The fault analysis tool can provide a reference for correct operation of conventional relays. To monitor the relay operations and improve the understanding of local information, event tree analysis (ETA) method is applied to provide a graphic monitoring tool for the relays responsible for clearing the disturbances. The detailed scheme of the local analysis method has been proposed in [12].

A. Neural Network Based Fault Detection and Classification (NNFDC)

An unsupervised/supervised based neural network algorithm for fault detection and classification is developed and described in [13]. An improvement of the original algorithm to solve particular application issues is proposed in [14]. The idea of this algorithm is discussed below.

With the continuous unsupervised/supervised training, the training patterns, which are formed from transient voltage and current signals, are allocated into groups (clusters) according to their similarity. The prototype and position of each cluster are then stored and used for recognizing and classifying unknown patterns.

The advantage of neural network based fault detection algorithm is that the neural network can form its “knowledge” by learning as many fault scenarios as it is presented and does not need to make compromise when determining settings as we do today when applying conventional distance relay schemes. With the approach, the accuracy of fault detection is improved under all circumstances.

B. Synchronized Sampling Based Fault Location (SSFL)

Fault location techniques are very important because they confirm whether a fault has indeed occurred on the line. By confirming the fault location result in the suspect disturbance area, we could determine which breakers are responsible to clear that fault, and unnecessary trips can be avoided or corrected to prevent spreading of the event.

Synchronized sampling based fault location algorithm is described in [15]. It takes the synchronized measurements from two ends of a transmission line to find an accurate fault point. Therefore, the algorithm does not depend on any assumptions about system operating conditions, fault resistance, fault waveforms, etc. In [16], it is proven that the algorithm has no problem to confirm the fault occurrence even during the power swing. In this sense, the SSFL algorithm can correct a possible misoperation of relay due to a power swing.

C. Event Tree Analysis (ETA)

Event tree analysis is a commonly used event/response technique in industry for identifying the consequences that can result following an occurrence of an initial event [17]. We can use it as an on-line monitoring tool for relay operations to indicate what happens as a consequence of a disturbance and what activities are taken by relays or other control methods.

An example of event tree analysis is shown in Fig.1. The node stands for the status after an event happened or an action is taken. The white ones represent correct actions and the black ones represent incorrect actions. Table I gives the explanation of the meaning of each node. The whole event tree should cover all possible activities following the root node (initial event). Finally, the actual event evolution path is monitored to see if the activities are approaching a final expected status. If not, a corrective action needs to be issued.

For a single distance relay, at least three event trees need to be built to match three types of initial events: (1) No fault detected in either primary zone or backup zones; (2) Fault detected in the primary zone; (3) Fault detected in backup zones. A design of the three kinds of event trees can be found in [12]. It should be noted that the design of the ETA is not unique. It should be carefully designed for each relay system, taking into account the detailed relay settings and system configurations.

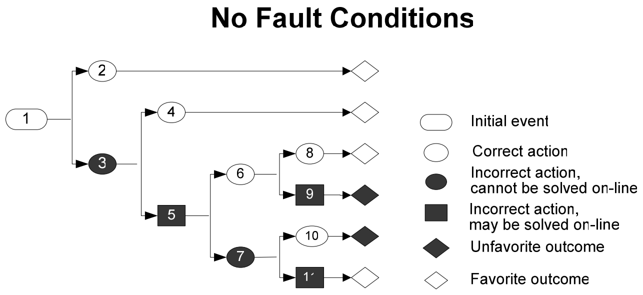

Fig. 1. Event tree for non-fault conditions

TABLE I
SCENARIOS AND REFERENCE ACTIONS FOR THE NODES OF THE EVENT TREE

Node	*Scenarios*	*Reference Action*
1	No fault in preset zones	Keep monitoring
2	Relay does not detect a fault	Stand by
3	Relay detects a fault	Check the defects in relay algorithm and settings
4	Trip signal is blocked	
5	Trip signal is not blocked	Send block Signal if necessary
6	Circuit breaker opened by the trip signal	
7	Circuit breaker fails to open	Check the breaker circuit.
8	Autoreclosing succeeds to restore the line	
9	Autoreclosing fails to restore the line	Send reclosing signal to the breaker
10	Breaker failure protection trips all the breakers at the substation	

11	No Breaker failure protection or it doesn’t work	Check the circuit of the breaker failure protection.

V. Interactive Scheme of the System as well as Local Monitoring and Control Tools

The block diagrams of relationship between the system analysis and local analysis are shown in Fig.2 and Fig.3.

The security analysis algorithm obtains power system information from measurements (i.e., SCADA) and runs the vulnerability analysis, as well as static and dynamic contingency analysis routinely. Vulnerability analysis evaluates the vulnerability of individual element and the whole system. Static and dynamic contingency analysis finds the contingencies which can lead to problems such as line overload, bus low/high voltage, angle stability, voltage stability, etc. The emergency control means will be chosen and used to mitigate such expected contingencies. The critical elements, which are more vulnerable to contingencies, or whose outages may threaten the system security, will be found based on the above analysis. This information will be sent to the local analysis for detailed monitoring.

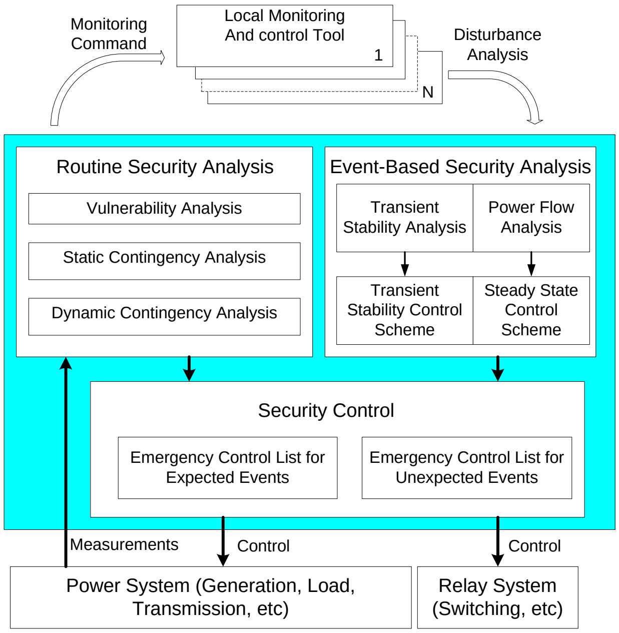
Monitoring Command
Local Monitoring And control Tool
1
N
Disturbance Analysis
Routine Security Analysis
Vulnerability Analysis
Static Contingency Analysis
Dynamic Contingency Analysis
Event-Based Security Analysis
Transient Stability Analysis
Power Flow Analysis
Transient Stability Control Scheme
Steady State Control Scheme
Security Control
Emergency Control List for Expected Events
Emergency Control List for Unexpected Events
Measurements
Control
Control
Power System (Generation, Load, Transmission, etc)
Relay System (Switching, etc)

Fig.2. Block Diagram of System Monitoring and Control

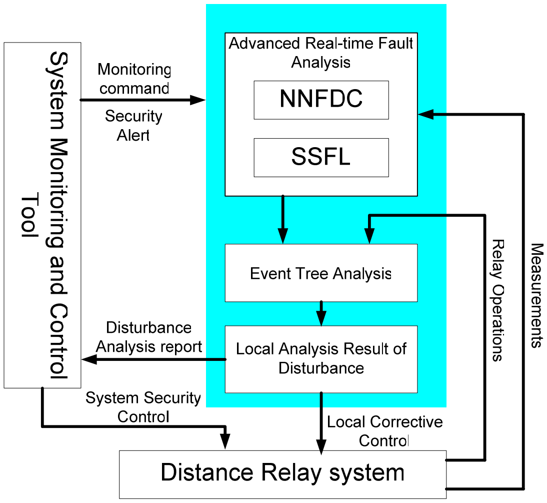

Fig.3. Block Diagram of Local Monitoring and Control

The local analysis tool serves as a backup on-line fault analysis tool using a combined NNFDC and SSFL algorithm. When a suspect disturbance is detected, either by relay or by the fault analysis tool, the local analysis tool will find the matching event tree according to the fault analysis result. Then the actual relay operations will be tracked in that event tree and finally the event sequence of that relay system will be obtained. This information will be sent to the system analysis tool for further system security analysis. The misoperations of relays can be corrected by local action quickly or mitigated by system security control after a detailed system-wide analysis.

System event-based analysis will get the disturbance information from system measurements and local analysis. If such events are studied by the routine security analysis, pre-determined emergency control means will be activated. If the events are unexpected, transient stability analysis and power flow analysis will be run to see whether there are transient stability or steady state problems. If so, associated control means will be found and issued to mitigate such events.

VI. Case Study

The IEEE 39-bus New England test system, as shown in Fig.4, is used to demonstrate the new approach. Detailed system data can be found in [18].

Case 1. Routine system security analysis

In this case, the system routine security analysis is implemented off-line and the vulnerable lines in the system are found. For those lines, the local analysis tool proposed in this paper needs to be installed to monitor the relays.

From topology processing, we find 11 lines from the one-line diagram shown in Fig.4: L22(B19~16), L47(B20~19), and 9 generator branches L37~L45 which connect G30~G38 respectively. There will be one or several buses isolated from the system if any of the above 11 lines are disconnected. The local analysis tools need to be applied on those lines.

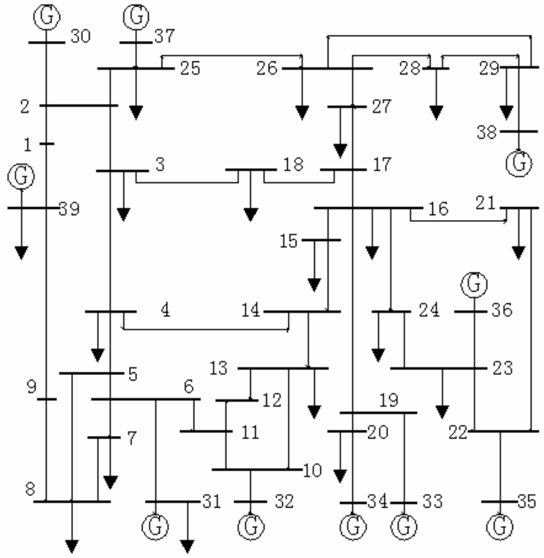

Fig.4. IEEE 39-bus System

By vulnerability analysis for distance relays (we assume all lines have distance relays), we find the top 6 most vulnerable lines according to their vulnerable indices as shown in Table II. For those lines, the fault on the neighboring lines may affect their relay operations. Therefore, those lines also need to be monitored using the local analysis tools.

Case 2. Event-based security analysis

In this case, it will be demonstrated how relay misoperation can cause system blackout. Then we describe how to prevent such situation with the benefit of the proposed interactive analysis approach.

The sequence of the scenarios is as follows:
1) t=0s, a 3-phase fault occurs at middle of L27(B22~21).
2) The fault is cleared at t=0.11s by tripping L27.
3) t=1s, a second 3-phase fault occurs at middle of L3(B3~2) and
4) The second fault is cleared at t=1.11s by tripping L3.

This contingency may cause relay at B24 of L29 (B24~B23) to misoperate. The trajectory of impedance seen by that relay is shown in Fig.5 with the event sequence labeled. The relay sees zone 3 fault at t=0.242s after the first fault clearing till t=1.008s the trajectory leaves zone 3 circle. Then the relay sees zone 3 fault again at t=1.520s. It may stay at the zone 3 circle longer than the setting time. The distance relay may trip L29 if zone 3 timer expires.

Thus, buses 22, 23, 35 and 36 will be isolated from the system, including the G35, G36 and load at B23, B24. The rest of the system is unbalanced and further cascading outage may happen.

This situation can be prevented by the interactive system and local analysis. From Table II, we can see L29 has already been placed on the vulnerable line list and the local analysis tool needs to be installed on that line. When the first fault occurs, the event-based system security analysis is activated. Through power flow analysis, it is determined that L29 is heavily loaded due to L27 outage. Also from the topology processing, it is determined that L29 and L27 are critical pairs. Therefore, through the system analysis, an alert signal will be sent to the local analysis tool at L29 to increase the security level. When the second fault happens, the local analysis tool draws a conclusion to block the relay from tripping for zone 3 fault. That information will be sent back to the system. The system will issue appropriate control means to mitigate the disturbances.

Table II. VULNERABLE LINES AND THEIR NEIGHBORING LINES

Line No	Bus Connection	VI_ Relay	Neighboring Lines (the contingency on those lines could influence the vulnerable line)
L37	B6~31	0.0240	L9(B6~5),L11(B7~6),L12(B11~6)
L38	B10~32	0.0206	L16(B11~10),L17(B13~10)
L42	B23~36	0.0191	L28(B23~22),L29(B24~23)
L45	B29~38	0.0157	L33(B29~26),L34(B29~28)
L43	B25~37	0.0149	L4(B25~2),L30(B26~25),L33
L29	B24~23	0.0131	L24(B24~16),L28,L42

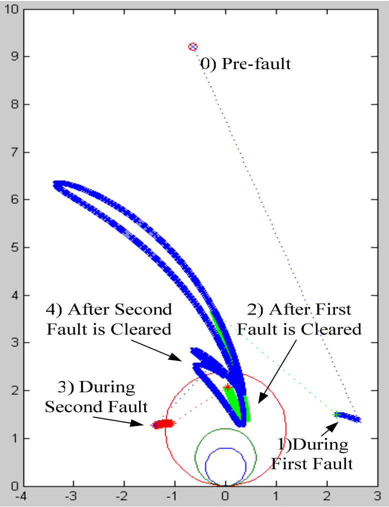

Fig.5. Apparent impedance seen by distance relay at L29(B24~23) during the 4s simulation period

In an actual large scale system, it is impossible that one or two contingencies like the ones discussed in this scenario can cause large scale system oscillation. Usually there is enough time for coordinating the system and local analysis to mitigate the disturbances before they unfold into the large one. An interactive system and local analysis approach can really help understand the disturbances and improve the security of system operations.

VII. Conclusion

Following conclusions can be drawn:

- New approach to prevent cascading outage can be obtained by the coordinated system and local tools.
- The system monitoring tool can find the vulnerable elements and send request to the local tool for detailed monitoring.
- Emergency control means for expected events can be found by the routine security analysis and activated when such events occur.
- Emergency control means for unexpected events can be found by event-based security analysis and activated to mitigate the disturbance and keep the system secure.
- The local monitoring tool can find the exact disturbance information and make a correction if there is relay misoperation. Further information can be sent to the system analysis for better security control.

VIII. References

[1] U.S.-Canada Power System Outage Task Force, “Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations”, April 5, 2004, Available: http://www.nerc.com

[2] NERC System Disturbances Reports, North American Electric Reliability Council, New Jersey, 1984-1991

[3] NERC Disturbance Analysis Working Group, “Western Interconnection (WSCC) System Disturbance — August 10, 1996”, NERC 1996 System Disturbances Report, Aug 2002, Available: http:// www.nerc.com

[4] Q. Chen, K. Zhu, J.D. McCalley, "Dynamic decision-event trees for rapid response to unfolding events in bulk transmission systems", in Proc. of IEEE 2001 Power Tech Proceedings, Vol. 2 , Sept 2001

[5] B.A. Carreras, V.E. Lynch, I. Dobson, "Dynamical and probabilistic approaches to the study of blackout vulnerability of the power transmission grid", in 2004 Proc. of the 37th Annual Hawaii International Conference on System Sciences, Jan. 2004, pp. 55 - 61

[6] J.C. Tan, P.A. Crossley, P.G. McLaren, "Application of a wide area backup protection expert system to prevent cascading outages", IEEE Transactions on Power Delivery, vol. 17(2), April 2002, pp. 375 - 380

[7] D. C. Elizondo, J. de La Ree, A. G. Phadke, S. Horowitz, "Hidden failures in protection systems and their impact on wide-area disturbances", in Proc. of IEEE 2001 PES Winter Meeting, Jan/Feb 2001, Vol. 2, pp. 710 – 714

[8] H. Song, M. Kezunovic, "Static Security Analysis based on Vulnerability Index (VI) and Network Contribution Factor (NCF) Method", IEEE PES T&D 2005 Asia Pacific, Dalian, China, Aug 2005

[9] M.A. Pai, P.W. Sauer, F. Dobraca, A new approach to transient stability evaluation in power systems, in Proc. of the 27th IEEE Conference on Decision and Control, Dec. 1988, vol.1, pp. 676 - 680

[10] H. Song, M. Kezunovic, "A Comprehensive Contribution Factor Method for Congestion Management", in 2004 Proc. of IEEE PES PSCE, Oct 2004

[11] H. Song, M. Kezunovic, "Stability Control using PEBS method and Analytical Sensitivity of the Transient Energy Margin", in 2004 Proc. of IEEE PES PSCE, Oct 2004

[12] N. Zhang, M. Kezunovic, "Verifying the Protection System Operation Using An Advanced Fault Analysis Tool Combined with the Event Tree Analysis," Northern American Power Symposium, NAPS 2004 Moscow, Idaho, August 2004.

[13] S. Vasilic, M. Kezunovic, "Fuzzy ART neural network algorithm for classifying the power system faults," *IEEE Trans. on Power Delivery*, vol. 20, no. 2, pp.1306-1314, April 2005.

[14] Nan Zhang, M. Kezonovic, "Coordinating fuzzy ART neural networks to improve transmission line fault detection and classification," IEEE PES General Meeting, San Francisco, June 2005.

[15] M. Kezunovic, B. Perunicic, and J. Mrkic, "An Accurate Fault Location Algorithm Using Synchronized Sampling," Electric Power Systems Research Journal, Vol. 29, No. 3, pp. 161-169, May 1994.

[16] Nan Zhang, M. Kezunovic, "A study of synchronized sampling based fault location algorithm performance during power swing," St. Petersburg PowerTech' 05, St. Petersburg, Russia, June 2005

[17] Jacobs Sverdrup Inc, System Safety and Risk Management Guide for Engineering Educators.
http://www.sverdrup.com/safety/riskmgt/lesson_9.pdf

[18] M. A. Pai, Energy Function Analysis for Power System Stability, Kluwer Academic Publishers, Norwell, MA, 1989, pp.222-227

IX. Biographies

Nan Zhang (S'04) received his B.S. and M.S. degrees from Tsinghua University, Beijing, China both in electrical engineering, in 1999 and 2002 respectively. Since Jun. 2002, he has been with Texas A&M University pursuing his Ph.D. degree. His research interests are power system analysis, power system protection, power system stability, system-wide disturbances, as well as signal processing and artificial intelligence applications in power systems.

Hongbiao Song (S'04) received his B.S. and M.S. degrees in electrical engineering from North China Electric Power University, China in 1999 and 2002, respectively, and currently is a Ph.D. candidate in electrical engineering at Texas A&M University. His research interests are power system analysis, simulation, protection, stability and control.

Mladen Kezunovic (S'77, M'80, SM'85, F'99) received his Dipl. Ing. Degree from the University of Sarajevo, the M.S. and Ph.D. degrees from the University of Kansas, all in electrical engineering, in 1974, 1977 and 1980, respectively. Dr. Kezunovic's industrial experience is with Westinghouse Electric Corporation in the USA, and the Energoinvest Company in Sarajevo. He also worked at the University of Sarajevo. He was a Visiting Associate Professor at Washington State University in 1986-1987. He has been with Texas A&M University since 1987 where he is the Eugene E. Webb Professor and Director of Electric Power and Power Electronics Institute. His main research interests are digital simulators and simulation methods for equipment evaluation and testing as well as application of intelligent methods to control, protection and power quality monitoring. Dr. Kezunovic is a registered professional engineer in Texas, and a Fellow of the IEEE.