Impact Assessment of Communication Service Disruptions in Power System Applications

Qi Wang, *Student Member*, *IEEE*, Manisa Pipattanasomporn, *Senior Member*, *IEEE*, Murat Kuzlu, *Senior Member, IEEE*, Yi Tang, *Member*, *IEEE*, Yang Li, *Member*, *IEEE*, and Saifur Rahman, *Fellow, IEEE*

***Abstract*—The communication system is the key element in an electric power system that supports its observability and controllability. Communication failures pose serious risks in electric power system operations. It is therefore crucial to study the adverse effects of communication system failures on power system operation. This is especially for wide-area monitoring, control and protection applications where rapid corrective actions are taken to prevent cascading failures. In this paper, a framework to evaluate the role of communication services on wide-area power system operation is proposed. A case study based on real-world power and communication systems is used to demonstrate usefulness of the proposed framework.**

***Index Terms*-- impact assessment, communication service, failure probability, wide-area network.**

I. Introduction

With the accelerated deployment of smart grid technologies and applications, a traditional electric power grid has become a complex system with integrated communications. A communication system is one of the most critical elements that support the observability and controllability of an electric power system. Classified by data rate and coverage range, a communication network can be classified into: Home Area Network (HAN)/Building Area Network (BAN)/Industrial Area Network (IAN), Neighborhood Area Networks (NAN)/Field Area Network (FAN) and Wide Area Network (WAN). The detailed principle of classification and characteristics of each class is described in [1]. In this paper, WAN is the focus. With protection, control and real-time wide-area monitoring applications supported in WAN, early stage of cascading faults in electric power systems can be effectively detected and prevented.

Communication faults, such as interruptions, high latency and data error, may lead to an electric power grid operating in its abnormal state that may propagate into cascading failures. In recent years, there have been several failure incidents in electric power systems that were caused by communication faults. These include incorrect actions of transmission system's protection devices caused by abnormally long latency and bit errors in communication channels in south China [2]; the blackout in south London in 2003 that was induced by erroneous alarm data [3]; and the expansion of "August 2003" blackout in USA and Canada for unobservable system status as a consequence of communication line interruption [4]. Therefore, it is of urgent need to investigate negative impacts of communication system disruptions/delays on wide-area power system applications.

Authors in [5] treated power and communication systems as a coupled, interdependent system based on a complex network theory. This kind of research method can be used to reveal the reason of cascading failures at the macro level, however, it cannot be directly adopted to guide operation and control of power systems for excessively ignoring their physical characteristics. Authors in [6] proposed a vulnerability assessment method to systematically evaluate supervisory control and data acquisition (SCADA) systems in the cyber security layer. Authors in [7] presented a quantified reliability evaluation method for wide-area measurement system (WAMS) with consideration of network structure and hardware reliability. Only specific communication services are considered in the above literature, and the impact of latency on power system operation is not well documented.

This paper presents a research framework to assess the impact of communication system faults on wide-area electric power system operation. Both reliability and vulnerability are discussed that can be used as indices to evaluate the weakness of the integrated power-communication system. This paper is organized as follows. The impact of communication service failures on wide-area power system applications are discussed in Section II. The impact assessment framework is presented in Section III. A case study to demonstrate the proposed framework is given in Section IV.

II. Impact of Communication Service Failures on Wide-Area Power System Applications

Monitoring, protection and control applications in a wide-area network usually require a large amount of data to be transmitted and received at high frequency (i.e., in a fraction of seconds) to support power system stability control. As a result, optical communication technologies that support high data rate (i.e., 10Mbps - 1Gbps) and provide long coverage distance are commonly used [1]. Based on real-world data from an electric utility, the structure of a wide-area power network and its corresponding WAN is shown in Fig. 1.

This work was supported by China Scholarship Council (File NO.20140690151) and State Grid Corporation of China project: Key Technologies for Power System Security and Stability Defense Considering the Risk of Communication and Information Systems.

Q. Wang, Y. Tang and Y. Li are with School of Electrical Engineering, Southeast University, Nanjing, Jiangsu, 210096 R.P.China (e-mail: wangqi@seu.edu.cn; tangyi@seu.edu.cn; and li_yang@seu.edu.cn).

M. Pipattanasomporn, M. Kuzlu, and S. Rahman are with are with Virginia Tech – Advanced Research Institute, Arlington, VA 22203 USA (e-mail: mpipatta@vt.edu; mkuzlu@vt.edu; and srahman@vt.edu).

978-1-4673-8040-9/15/$31.00 ©2015 IEEE

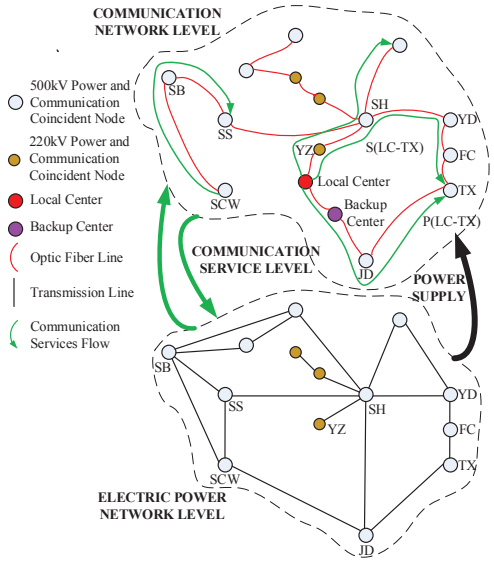

Fig. 1. Structure of regional power and communication networks from an electric utility in the south area of Jiangsu province, China.

In general, most major physical electric power nodes (e.g., nodes SCW and SS in the electric power network level) usually have their corresponding communication facilities, which are shown as communication nodes (e.g., nodes SCW and SS in the communication network level). However, the connection between two nodes in each level may not be the same. For example, the power nodes SCW and SS have a physical connection, while the information from node SCW to SS is transmitted through node SB. Note that the local control center node and the backup control center node in the communication network level generally do not have corresponding power nodes.

Table I summarizes the impact of communication service failures on operation of different wide-area applications.

TABLE I
Classification of communication services and consequence of failure

Application Service	Consequence of Failure
Wide Area Protection Service	
Adaptive islanding Predictive under frequency load shedding Wide area relay protection	mal-operation rejecting operation
Wide Area Control Service	
Wide-area voltage stability control FACTS and HVDC control Cascading failure control Precalculation transient stability control Closed-loop transient stability control Wide-area power oscillation damping control	mal-operation rejecting operation inaccurate operation
Wide Area Monitoring Service	
Wide-area power oscillation monitoring Wide-area voltage stability monitoring PMU-based state estimation Dynamic state estimation PMU-assisted state estimation	declining objectivity declining controllability

Wide area protection service protects power systems against widespread blackouts, transmission congestion and stressed conditions, or other unexpected events. Failures of communication services may cause mal-operation of devices or devices rejecting operation, which may lead to unnecessary load loss and even more catastrophic damages.

Wide area control service provides automatic self-healing capabilities that exceed functionalities delivered by local control and responds faster than manual control by a control center. Although mal-operation or rejecting operation of devices can happen with communication faults, their impacts can be minimized by having a back-up local and off-line controls. Thus, consequences can include inaccurate operation.

Wide area monitoring service aims at providing system data in real-time from a group of intelligent electronic devices (IEDs) and phasor measurement units (PMUs). Although failure of communication services may not cause direct consequences, it will reduce system objectivity and controllability.

III. Impact Assessment Framework for Wide-Area Power System Applications

The framework of impact assessment proposed in this study is illustrated in Fig. 2.

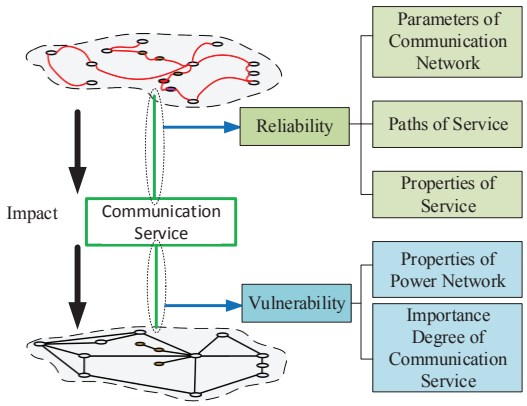

Fig. 2. The proposed impact assessment framework.

As shown, reliability and vulnerability of communication services are taken into account. In this study, reliability is defined as the probability of a communication service to perform a required function successfully under a given communication network structure and operating conditions [8]. This reliability is assessed based on parameters of communication networks (i.e., latency and failure probability of communication nodes and lines), paths of service (i.e., primary path or backup path) and the properties of services (i.e., data transmission latency requirement). Vulnerability is defined as the consequence of communication service failures and can be assessed based on properties of a power network (i.e., importance index of power nodes) and importance degree of each communication service. The approach to perform reliability and vulnerability assessment of the power network with integrated communications is discussed below.

A. Reliability Assessment

In the proposed framework, reliability of a communication system is assessed based on available communication path(s) and transmission latency. Data are usually transmitted from one communication node to the other through either a primary path or a standby path, depending on their availability. Fig. 3

illustrates possible data transmission paths between the two communication nodes, assuming that the information is transmitted from the local center (LC) to the destination node YB. In this case, the primary data transmission path is P(LC-YB) as shown in State 1; and the standby paths are S_1(LC-YB), S_2(LC-YB) and S_3(LC-YB) as shown in State 2.

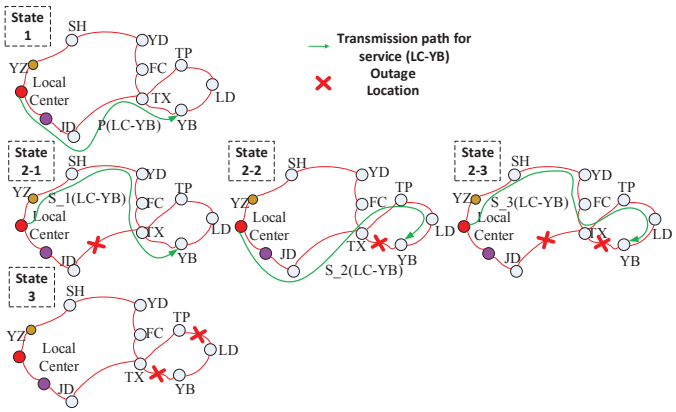

Fig. 3. States of service between two communication nodes.

As shown, three possible states of communication paths are discussed below:

State 1 - Primary path remains in its working state: This is a normal operating state when all components in the primary path are available, as shown in Fig. 3. The probability of adopting the primary path is formulated as the product of component availability:

$$P_{\mathrm{P}}\left(S_n^{mn}\right)=\prod_{N_{cj},B_{ci}\in Path_P\left(S_n^{mn}\right)}\left[1-P\left(I_{bci}\right)\right]\left[1-P\left(I_{ncj}\right)\right] \quad (1)$$

where:

S_n : the n^{th} kind of communication service
S_{n}^{mn} : the $m_{\mathrm{n}}{}^{\text{th}}$ service of S_n
$Path_{\mathrm{P}}(S_{\mathrm{n}}^{mn})$: the primary paths of service $S_n{}^{mn}$
$P(I_{\mathrm{bci}})$: the interruption probability of line b_{ci}
$P(I_{\mathrm{ncj}})$: the interruption probability of node n_{cj}

State 2 – An outage occurs only in the primary path: This is shown as states 2-1, 2-2 and 2-3 in Fig. 3. The adoption of a standby path happens with the outage of a corresponding primary path. For example, when an outage occurs in the path LC-JD-TX, only S_1(LC-YB) will be adopted although S_3(LC-YB) is also available. A successful auto-switching operation is needed in this state. The probability of adopting each standby path is formulated as the product of component unavailability in the corresponding parallel primary path and the availability of components in standby path as:

$$P_{S\_k}\left(S_n^{mn}\right)=\prod_{x=1}^{X}\left\{1-\prod_{N_{cj},B_{ci}\in Path_{P\_k-x}\left(S_n^{mn}\right)}\left[1-P\left(I_{bci}\right)\right]\left[1-P\left(I_{ncj}\right)\right]\right\} \times\prod_{N_{cj},B_{ci}\in Path_{S\_k}\left(S_n^{mn}\right)}\left[1-P\left(I_{bci\_s}\right)\right]\left[1-P\left(I_{ncj\_s}\right)\right] \quad (2)$$

where:

$Path_{P\_\mathrm{k}\text{-}\mathrm{x}}(S_{\mathrm{n}}^{mn})$: the x^{th} part of primary path which in interruption state
k : the standby path serial number
X : the total number of interruption events occurred in $Path\_k$
$Path_{S\_\mathrm{k}}(S_{\mathrm{n}}^{mn})$: the corresponding standby path

State 3 – An outage occurs in both primary and standby paths: This is illustrated as state 3 in Fig. 3. The probability of this state, which can also be interpreted as interruption probability, is calculated as:

$$P_I\left(S_n^{mn}\right)=1-P_P\left(S_n^{mn}\right)-\sum P_{S\_k}\left(S_n^{mn}\right) \quad (3)$$

Interruption of all available paths will definitely cause the communication service to fail. Note that in states 1 and 2, the communication service can also fail if high latency is experienced. Each communication service has different requirements of data transmission latency, or a latency threshold value. When the data transmission latency of a communication path exceeds a threshold value, selected WAN services cannot be performed. For example, late reception of a control signal to a relay can cause blocking of relay protection equipment. Higher latency is likely to cause more adverse effect to power system operation. To quantify this kind of an impact, this paper considers latency of paths as a probability distribution function. This probability distribution function can be obtained from the historical data of the communication network of interest.

Based on path availability and factoring in the latency parameter, the overall reliability of a communication service S_{n}^{mn} is calculated by summing the probability of path availability in states 1 and 2 as:

$$P_R\left(S_n^{mn}\right)=P_P\left(S_n^{mn}\right)\times P_{P\_S_n^{mn}}\left(t<T_{S_n^{mn}}\right) +\sum_{k=1}^{K}\left[P_{S\_k}\left(S_n^{mn}\right)\times P_{S\_k\_S_n^{mn}}\left(\left(t+t_{switch}\right)<T_{S_n^{mn}}\right)\right] \quad (4)$$

where

K : the total number of standby paths
$T_{S_{\mathrm{n}}^{mn}}$: the threshold value of service S_{n}^{mn}
t : the latency of service path
$P_{P\_S_{\mathrm{n}}^{mn}}(*)$: the distribution function of service latency when being transmitted in primary paths
$P_{S\_k\_S_{\mathrm{n}}^{mn}}(*)$: the distribution function of service latency when being transmitted in standby paths

The distribution function of service latency can be calculated using the distribution function of the components through which the service is transmitted. Latency of each component can be described as a Gaussian distribution, and the parameters can be derived using real data.

B. Vulnerability Assessment

In this paper, the vulnerability of each communication service S_{n}^{mn} is obtained by multiplying the importance index (I_{pi}) of a power node with the importance degree (I_{Sn}) of each kind of service as follow:

$$V\left(S_n^{mn}\right)=I_{pi}\times I_{Sn} \quad (5)$$

The importance index I_{pi} of node N_{pi} in power system is determined using (6):

$$I_{pi}=\left(\frac{P_{LOL}^{N_i}}{P_{Total}}\right)^{L_{N_i}-1} \quad (6)$$

where

$P_{LOL^{Ni}}$: the load loss (MW)
P_{Total} : the total system load (MW)
L_{Ni} : the loading level at the node N_i

At the value L_{Ni}, the power flow diverges which is an indication of a severe impact. The more detailed calculation algorithm can be found in [6]. Importance degree I_{Sn} of each kind of service can be evaluated from communication system requirements. These requirements include: signal delay, bit error, net bandwidth, protection channel and security. Fuzzy Analytic Hierarchy Process (FAHP) method based on expert scoring is adopted to get weight of each attribute [10].

IV. Case Study

A case study based on the IEEE 30 bus test system, as shown in Fig. 4, is used to demonstrate the proposed impact assessment framework. A corresponding communication network is modeled based on properties of real-world WAN.

A. The Communication Network Model

The communication network model for the IEEE 30 bus test system is developed as shown in Fig. 4(b). It combines one backbone network (SDH-BN) and three regional networks (SDH-1, SDH-2 and SDH-3), all of which are self-healing ring network structure. Power system nodes (N_{pi}) are labeled as numbers 1-30 in Fig. 4(a). Corresponding communication nodes (N_{ci}) are labeled in square boxes in Fig. 4(b). Numbers on each communication paths represent distance of optical fiber lines in kilometers.

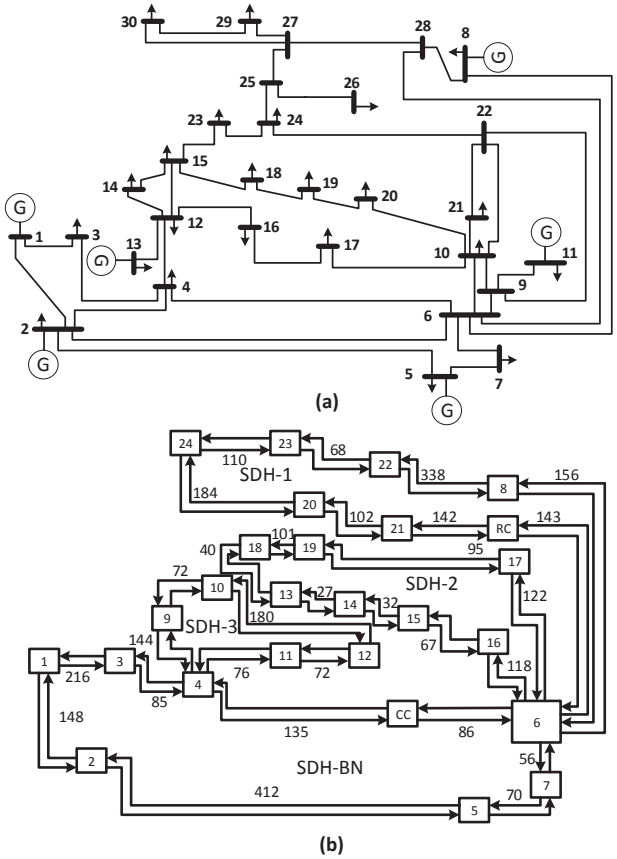

Fig. 4. (a) IEEE 30-bus test system; (b) Corresponding communication network of the IEEE 30-bus test system (CC-Control Center, RC-Regional Center).

The relationship between power and communication networks is shown in Table III. Importance index of each power node (I_{pi}) is calculated using (6).

TABLE III
Importance indices and vulnerability value of power nodes

N_{ci}	N_{pi}	I_{pi}	N_{ci}	N_{pi}	I_{pi}	N_{ci}	N_{pi}	I_{pi}
1	1	.0016	9	14	.0015	17	22	0
2	2	.1769	10	15	.0019	18	23	.0010
3	3	.0014	11	16	.0017	19	24	.0029
4	4,12,13	.3971	12	17	.0031	20	25	0
5	5	0	13	18	.0002	21	26	.0008
6	6,9,10,11	1	14	19	.0034	22	27,28	1
7	7	.0222	15	20	.0002	23	29	.0004
8	8	.0083	16	21	.0222	24	30	.0056

The data on interruption probability for communication components is obtained from [9], while the latency data is obtained from an electric utility, as shown in Table II.

TABLE II
Interruption and latency data for communication components

Network Unit	Interruption Data			Time Delay Data	
	FIT [a] *Rate*	*MTTR* [b] *(hours)*	*Interruption Probability* [c]	*Mean Time*/ms	*Standard Deviation*/ms
Node	8000	4	$3.2*10^{-5}$	0.4	0.04
Branch (/ km)	300	24	$7.2*10^{-6}$	$5*10^{-3}$	$4.17*10^{-4}$

a. 1 *FIT* is equivalent to the failure rate of 1 failure per 10^9 hours.
b. *MTTR* = mean time to repair (hours)
c. Interruption Probability=(*MTTR***FIT*)/10^9

B. Impact Assessment Results of Communication Services

Four WAN applications from Table I are selected for the impact assessment: relay protection service (S_1), closed-loop transient stability control service (S_2), PMU-based state estimation service (S_3) and wide-area voltage stability monitoring service (S_4). For this study, it is assumed that the number of services available are 64, 31, 24, and 17, for S_1, S_2, S_3 and S_4, respectively. It is also assumed that the threshold latency value of these services are 5ms, 15ms, 10ms and 30ms for S_1, S_2, S_3 and S_4, respectively. It is necessary to mention that the threshold value considered here is only transmission latency instead of the total time delay from a service being issued to a service being executed.

Table IV summarizes resulting reliability and vulnerability values calculated based on Eq. (1)-(6). The importance index (I_{Sn}) is calculated based on the FAHP method.

TABLE IV
Reliability and vulnerability results

Service	*Mean* P_R [a]	*Mean* P_I [b]	*Mean* P_T [c]	I_{Sn}	*Mean* V [d]
S_1	0.9988	$1.07*10^{-5}$	$1.14*10^{-3}$	0.3480	0.0992
S_2	0.9999	$6.97*10^{-5}$	$1.81*10^{-7}$	0.2404	0.0362
S_3	0.9998	$4.59*10^{-5}$	$1.61*10^{-4}$	0.2384	0.0507
S_4	0.9999	$8.13*10^{-5}$	0	0.1731	0.0191

[a] P_R is reliability value calculated using Eq. (4); [b] P_I is interruption probability calculated using Eq. (3); [c] P_T is outage probability calculated as $1-P_I-P_R$; and [d] V is vulnerability value calculated using Eq. (5).

All services have a reliability value (P_R) above 99.8%,

which means, in a normal condition, these communication services are highly reliable.

Interruption probability (P_I) of a service is related to the transmission path and interruption probability of components in this path. For being mainly transmitted between two neighboring nodes, relay protection services have lowest mean interruption probability.

While the outage probability (P_T) of a service is related to the threshold latency value and the distribution function of latency in relevant transmission paths. Because of the lowest threshold value, relay protection services have relatively high P_T. On the other hand, wide-area voltage stability monitoring services have the lowest P_T.

Relay protection services also have high mean vulnerability, followed by PMU-based state estimation services and closed-loop transient stability control services. In actual operation, service with high vulnerability should get extra attention.

C. Impact of WAN with Faults

To study changes in reliability value (P_R) with a communication interruption, this study considers two interruption scenarios: (1) an interruption occurs in communication line 4-9; and (2) an interruption occurs in communication line 6-CC. The changes in service reliability are shown in Table V.

TABLE V
Changes in reliability value (P_R) with communication interruptions

Scenario	*Average Decline of Reliability*	*Number of Services with Reliability<0.95*	*Number of Services with Reliability<0.1*
1 (line 4-9)	$2.56*10^{-4}$	0	0
2 (6-CC)	0.0487	7	5

Reliability of services in scenario 1 has a slight decline, but the whole system still stays in an acceptable safety range as all available services have reliability values greater than 0.95. While in scenario 2, for line 6-CC being the key path to system control center, its interruption causes more serious consequences. As shown in Table V, seven (7) services out of all available services have reliability value less than 0.95, and five (5) services have reliability value less than 0.1, implying that they have an extremely high chance of failure. These include, for example, relay protection services between nodes 4-6 and 12-6, and PMU-based state estimation services between nodes 18-CC. This kind of study can be used to obtain the most critical components in communication network.

D. Dynamic Variation of Reliability

Assume latency of communication node 6 increases 0.1 ms every 30 minutes. The dynamic variation of reliability value of services is shown in Fig. 5. With time increasing, the reliability values of several relay protection services (i.e., services between 6-2, 6-1 and 6-22, which are shown as S_1 (6-2), S_1 (6-1), S_1 (6-22), respectively), drop sharply. This later on leads to a complete failure of these services. Note that, the reliability values of other services are insignificantly impacted by increasing latency overtime. The dynamic variation of reliability of all services can be used to expose the most unreliable communication services in the power system during its operation.

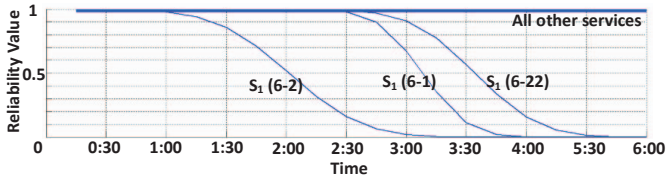

Fig. 5. Dynamic variation of reliability when latency of communication node 6 increases 0.1 ms every 30 minutes.

V. Conclusion

The integration of the communication system with electric power system operation has brought about brand-new challenges. This paper presents the impact assessment framework to evaluate reliability and vulnerability of communication services on power system operation. The IEEE 30 bus system with its corresponding communication system is adopted as an example to illustrate the assessment method. Assessment results can provide key information for identification of the weakness of integrated communication-power systems in both system planning and operation levels.

References

[1] M. Kuzlu, M. Pipattanasomporn, and S. Rahman, "Communication network requirements for major smart grid applications in HAN, NAN and WAN," Computer Networks, vol. 67, pp. 74-88, July 2014.

[2] X. Shen，Z. Shu and Y. Liu, et al, "Statistics and Analysis on Operation Situation of Protective Relayings of State Grid Corporation of China in 2009," *Power System Technology*, vol. 35, pp. 189-193, February. 2011.

[3] M. Amin, "Power system infrastructure security and defense," in *Proc. 2004. IEEE Power Engineering Society General Meeting*, pp.7-8.

[4] G. Andersson, P. Donalek and R. Farmer, et al, "Causes of the 2003 major grid blackouts in North America and Europe and recommended means to improve system dynamic performance," *IEEE Trans. on Power Systems*, vol. 20, pp. 1922-1928, October 2005.

[5] S. V. Buldyrev, R. Parshani and G. Paul, et al, "Catastrophic cascade of failures in interdependent networks," *Nature*, vol.464, pp. 1025-1028, April 2010.

[6] C. Ten; C. Liu and G. Manimaran, "Vulnerability Assessment of Cybersecurity for SCADA Systems," IEEE Trans. Power Systems, vol. 23, pp.1836-1846, November. 2008.

[7] Y. Wang, W. Li and J. Lu, "Reliability Analysis of Wide-Area Measurement System," *IEEE Trans. Power Delivery*, vol.25, pp.1483-1491, July 2010.

[8] J. Johansson, H. Hassel and E. Zio, "Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems," *Reliability Engineering & System Safety*, vol. 120, pp. 27-38, December 2013.

[9] A. Antonopoulos, J. J. O'Reilly and P. Lane, "A framework for the availability assessment of SDH transport networks," *in Proc. 1997 2nd IEEE Symp. Computers and Communications*, pp. 666–670.

[10] L. Mikhailov, P. Tsvetinov, "Evaluation of services using a fuzzy analytic hierarchy process," *Applied Soft Computing*, vol. 5, pp. 23-33, December 2004.