Journal of Power and Energy Engineering, 2015, 3, 77-84
Published Online April 2015 in SciRes. http://www.scirp.org/journal/jpee
http://dx.doi.org/10.4236/jpee.2015.34012

Analysis of Causes and Actual Events on Electric Power Infrastructure Impacted by Cyber Attack

Hongxu Yin[1], Rui Xiao[2], Fenfei Lv[1]

[1]The Power Company of Dezhou, Shandong, Dezhou, China
[2]College of Mechanical & Electrical Engineering, Jiaxing University, Jiaxing, China
Email: hongxu_yin@126.com

Received January 2015

Abstract

With the development of electric power technology, information technology and military technology, the impact of cyber attack on electric power infrastructure has increasingly become a hot spot issue which calls both domestic and foreign attention. First, main reasons of the impact on power infrastructure caused by cyber attack are analyzed from the following two aspects: 1) The dependence of electric power infrastructure on information infrastructure makes cyber attack issues in information field likely to affect electric power field. 2) As regards to the potential threat sources, it will be considerably profitable to launch cyber attacks on electric power infrastructure. On this basis, this paper gives a classified elaboration on the characteristics and the possibilities of cyber attacks on electrical infrastructures. Finally, the recently published actual events of cyber attacks in respect of threat sources, vulnerabilities and assaulting modes are analyzed and summarized.

Keywords

Cyber Attack, Electric Power Infrastructure, Information Infrastructure, Dependence

1. Introduction

Electric power infrastructure provides public power supply services for social production and household use. Recently, with the development of computer and communication technology, information and communication systems become an essential part to support the normal operation of electric power infrastructure. According to the relevant standards set by International Electro-technical Commission (IEC), the future development of power system will be the common construction and management of electric power infrastructure and information infrastructure [1].

Cyber attack takes advantage of network vulnerability and security flaw to attack on system and resources [2]. For power system, monitoring and communication equipment of electric power infrastructure are the direct target of cyber attack. But because of the electric power infrastructure's dependency on information infrastructure, cyber attack will affect the safe and and stable operation of power system [3] [4]. In view of the importance of

How to cite this paper: Yin, H.X., Xiao, R. and Lv, F.F. (2015) Analysis of Causes and Actual Events on Electric Power Infrastructure Impacted by Cyber Attack. *Journal of Power and Energy Engineering*, **3**, 77-84.
http://dx.doi.org/10.4236/jpee.2015.34012

electric power infrastructure and cyber attack's characteristics of low cost, wide range and hidden action [5], cyber attack will become a potential threat that we may not neglect [4] [6]-[8].

Currently, many countries, mainly the U.S., have raised the impact of cyber attack on electric power infrastructure to nation-state level. The Homeland Security Department（DHS）has organized three cyber storm exercises since 2006 to 2010, and electric power infrastructure are significant imaginary target [9]. An Israeli-US strike on Iranian nuclear plants [10] becomes the focus of the international concern in 2011. According to this development trend, cyber attack on electric power infrastructure will be an important means of network information war [11], which needs to be paid high attention and intensive study.

This paper is organized focusing on the impact on power infrastructure caused by cyber attack. And the background and current situation of the problem are discussed to draw attention of national related departments, enterprises and research institutes. This paper analyses main reasons of the impact on power infrastructure caused by cyber attack, and summarizes characteristics of existing cyber attack. Furthermore, the impact of recently published actual events of cyber attacks on electric power infrastructure is analyzed.

2. Main Reasons of the Impact on Power Infrastructure Caused by Cyber Attack

2.1. The Dependence of Electric Power Infrastructure on Information Infrastructure

According to the IEC standards above, the power system can be divided into two parts, electric power infrastructure and information infrastructure. Electric power infrastructure, often called power primary system, is composed of power generation, transmission, transformation and distribution equipment, and its function is to lower the voltage of electrical energy generated step by step by transmission and transformation equipment and then transfer the electrical energy to distribution system. At last the electrical energy is supplied to customers through distribution line. Information infrastructure, usually called power secondary system, is composed of power monitoring system, power telecommunication, data network, etc. Power monitoring system are the business processing systems and smart devices based on computer and network technology, whose function is to monitor and control the production and operation process of the power grid and power plants [12].

The construction and development of information infrastructure are natural products of the development of communications and information technology, and also the objective requirements of the development of power system to a certain degree, aiming to improve the safety and economy of power system operation.

Interdependence of infrastructures is the interrelation or influence of the unions of 2 infrastructures. Generally, this dependence can be divided into 4 types [13]. The first type is physical dependence, which refers to the physical dependence existed between the unions of 2 infrastructures in the form of material flow. The second one is information dependence, which refers to the information dependence existed between the unions of 2 infrastructures in the form of information flow. The third one is geographical dependence, which means that the unions of 2 infrastructures are adjacent geographically and the incident in this site may affect both of the infrastructures. The last one is logic dependence, which means that the dependence exists between the unions of 2 infrastructures, but it can't be attributed to any of interdependence relationships discussed above.

Cyber security is the negative factors existed in information infrastructure, and severity of its influence on electric power infrastructure depends on the electric power infrastructure's dependence on information infrastructure.

Generally, the units of electricity power infrastructure can be divided into three classes, namely plants, substations, and lines, which constitute the entire electricity network. Information infrastructure, as it provides service to electric power infrastructure, exists in power plant monitoring system and substation automatic system corresponding to the units above. These systems mainly satisfy the units' own needs with a relatively small service scope, and they can realize local automation function, such as protection and operation and control functions based on station control level.

From a global perspective, the operating state of power system is adjusted based on the variation of load. So it is necessary to acquire global monitoring information and adjust generator's output power reasonably according to the variation of load to ensure safety and economic operation of the system. These functions are based on local function, and realized by supervisory control and data acquisition/energy management system (SCADA/EMS).

The growth of load and scale expansion of power grid proposes a higher request of safety, promoting the development of wide area measurement and protection control system. The realization of wide area measurement

and protection control system is also based on the collection, analysis and control of global information. Compared with SCADA/EMS, this requires more information and higher real-time character [14]-[16]. To satisfy the demand for uninterrupted power supply, it is essential to ensure the safety operation or instant recovery of information infrastructure when suffering internal fault or external attack [17]. The impact of information infrastructure on electric power infrastructure will be negative if the monitoring can't be conducted real-time or being taken advantage of.

In summary, information infrastructure serves electric power infrastructure in power system. In turn, electric power infrastructure depends on information infrastructure. The dependence's working point is substation automatic system or power plant monitoring system, but is amplified through the function of SCADA/EMS and wide area measurement and protection control system.

2.2. The Concept of Cyber Attack and Motivation Analysis

2.2.1. The Concept of Cyber Attack

According to the concept in the field of information security, cyber attack takes advantage of loophole and security vulnerabilities existing in the network to attack on system and resources.

Information infrastructure serving the power system to a great extent belongs to typical industrial control system. Cyber attack specified to those systems is generally defined as attack on the behavior of computer-based industrial control system without permission, aiming at destroying or lowering the function of industrial control system [18].

According to the physical security and network security guidelines of substation established by IEEE, cyber attack specified to substation refers to invading substation through possible network and operating or interfering with electronic equipment [19]. Equipment operated or interfed with include digital relay protection devices, fault recorder, automatics, substation-control level computer, PLC and communication interfaces [6].

2.2.2. The Benefit of Cyber Attack

Motivation of cyber attack derives from the aggressor's increasing economic or political interests. Compared with the traditional physical attack, cyber attack features with hidden action, low cost and wide range [5]. Cyber attack can implement aggressive behavior from any access network point of information infrastructure without approaching physical device. An attacker needs only relevant knowledge of the network and not special funding. Once an attack on electric power monitoring equipment implemented, some primary system equipment operate, possibly resulting in power system cascading failure and has larger influence sphere.

2.2.3. Threat Sources of Cyber Attack

Combined IEC 62351 standard [20] and reported domestic and international cyber attack, threat sources of cyber attack includes the following types.

1) Industrial espionage

Industrial espionage is becoming a major threat in higher power system marketization countries. Competition between enterprises increases motivation of illegal acquisition of information. And it is possible to interfere the operation of the competitors' equipment and improve their earnings.

2) Cyber hackers

Hackers usually take the Internet as a major gateway to attack, and gain profit by destroying cyber security. The profit may be monetary, industrial, political, social or the curiosity that whether the challenge of intrusion network will be successful [21].

3) Viruses

Similar to hackers, viruses and worms are typical attack taking advantage of the Internet. However, some viruses and worms may spread to Internet-isolated system by embedding into software or removable storage device. These viruses include middle attacks viruses, spyware gaining power system data and other trojan horse.

4) Larceny

Larceny has the most immediate purpose, namely attacker taking something (such as equipment, data or knowledge) away without permission. Generally speaking, the main motivation is to obtain economic benefits. Under the smart grid environment, the interaction of grid operators and user is emphasized. To tamper energy metering data through cyber attack is likely to develop into a new way of stealing electric power [22].

5) Terrorism

Terrorism is a threat which has minimum probability of occurrence. But it may bring serious consequences due to the purpose of maximizing the physical, financial, social and political damage.

6) Military action

Due to its specificity, electric power infrastructure is always taken as a priority target for military action. For example, US Army used graphite bombs to destroy the power system in Gulf War and the Kosovo War [23]. In recent years, with the mode and destructiveness of cyber attack increasing, physical attack gradually fades out of sight. And electric power infrastructure has become a potential target of cyber attacks, drawing military's attention [11].

3. Cyber Attacks against Electric Power Infrastructure

3.1. Classified by the Location of Attack

Depending on different location of cyber attack, attack can be classified as local attack, remote attack and pseudo remote attack.

Local attack occurs in the LAN, and remote attack occurs outside the location of the network the target belongs to. Pseudo remote attack is an attack that internal personnel covering up the identity of their attacker gain necessary information about the target from local and attack from the external, causing external invasion phenomenon [24].

Local attack needs to be physically close to the target. But local electric power monitoring system (e.g. Substation Automation System) usually adopt perfect physical isolation means, so it is difficult for attacker to reach the target, let alone attack. Remote attack can invade computers in control center and other critical equipment through any network connected to the power of information and communication network, utilizing the system vulnerabilities and unsound security and confidentiality mechanisms. In comparison, remote attack is most likely to occur [25]. Pseudo remote attack needs spies in power company, so it is less likely to occur.

3.2. Classified by Attack Mechanism

According to the mechanism, attack can be classified as denial service attack, replay attack, middle attack and reprograming the device [26].

1) Denial service attack (Dos)

Denial service attack occurs when excessive communication resources are occupied by an attacker so that the resource is temporarily unavailable when user needs to access, effecting the availability of information. In attacks against electric power infrastructure, attacker keeps sending forged packets in the communication channel, making the normal communication between the control center and RTU unavailable. The control center can't receive the power terminal information transmitted by RTU, meanwhile the control information issued by the control center can't be delivered. If the grid is in a state of emergency at the moment, the consequences would be unimaginable.

2) Replay attack

For replay attack, it is necessary to monitor network information flow first, and identify information representing key actions. The information is sent back into the network at specific times to re-simulate the previous occurrence. In electric power infrastructure, attacker can identify and intercept breaker tripping control instruction by network monitoring and replaying this instruction when necessary, resulting in breaker malfunction.

3) Middle attack

Attacker' action is imposed between two communicating nodes, and it deceives the sender that it is a true recipients or the recipients that it is the real sender. In this way, the attacker can tamper, delete or insert arbitrary information between two communicating nodes. In electric power infrastructure, attacker can be a middleman between RTU and control center, which intercept emergency fault information sent by RTU and replace with normal or alarm information, so that system does not take action in case of failure. Besides, it intercept control instruction from control center and delete, modify or insert the instruction. After such an attack, the confidentiality and integrity of information is completely lost. If the attacker is well aware of the power system operating state, then this attack would be devastating.

4) Reprograming the device

If RTU, IED and other equipment are reprogrammed, the attacker can easily implant malicious Trojans, disrupting the normal operation of equipment. This kind of attack is not common at present. The reasons mainly lie in two aspects: a) Remote programming of equipment is not allowed in the design of system generally, and local invasion programming needs approaching the equipment. But if the equipment is available, direct physical damage will be easier than reprogrammed and the destruction is more severe; b) As the equipment is numerous and geographically distributed, reprogramming attack is not suitable to launch a massive attack, and the requirement of programming capabilities of attacker is higher.

With the development of technology, the likelihood of such an attack still exists. For example, IEC 61850 standard proposes that IED equipment can be remotely configured [27]. Under the background of digital substation widely used and open of remote configuration interface in the future, such an attack would be more practical.

4. Case Study of Cyber Attack against Electric Power Infrastructure

4.1. Cyber Attack Instance

In recent years, cyber attacks on the Internet have been very serious, but reports about cyber attacks against electric power infrastructure are relatively few. Overall, the power monitoring system suffering from cyber attacks are on the rise. Some studies suggest that the current reported cyber attacks are likely just the tip of the iceberg. Due to fear of responsibility and corporate image damage, as well as commercial competition and other issues, most companies are reluctant to report such incidents [28]. Some examples of cyber attacks against electric power infrastructure are summarized as follows.

1) In the 8 - 14 blackout in USA and Canada in 2003, worm hindered the recovery from power blackout in Ontario in Canada to normal power supply [29].

2) In March 2007, U.S. Department of Defense and Department of Homeland Security (DHS) conducted a cyber attack experiment, causing generator self-destruction. The experiment was undertaken by the Idaho National Laboratory (INL) of energy, and it simulated a cyber attack against the copy of Aurora plant's control system. The attack invaded SCADA system and changed the generator's operation trajectory. Then the generator was out of control and galloping, final smoking and damaged. DHS believes that this type of cyber attack, if taking large-scale coordinated control, can damage electric power infrastructure for months. And DHS is reluctant to disclose specific details of the simulation action [30] [31].

3) On October 16, 2007, cyber security expert Ira-Winkler published a paper on the Internet Evolution site entitled "How to take down the power grid". This paper points out that it is not difficult to conduct cyber attack against power information control system, and he entered into American power control system as early as ten years ago. Ira-Winkler and his team have been hired by a power company, conducting test and evaluation of the vulnerability of computer systems for power grid. They can damage the browser, intrude into the control network of the power plant and monitor the power production and distribution, thus simulating the effects on the normal operation of the electric power infrastructure. Ira-Winkler noted that they can not only enter into SCADA system, but also download the file record CIO and CEO via cyber attack [4].

4) U.S. Central Intelligence Agency (CAI) pointed out that the blackout, which occurred in 2005 and 2007 in Brazil, was due to hacker's cyber attack against the power control system [32].

5) In an on-line special report of U.S. Public Broadcasting Company (PBS), an interviewee signatured hacker claimed that he could make the grid collapsed by clicking on some buttons. It is important that hackers, vandals and terrorist attackers think it is possible, not the truth of this sentence. And this report reflects that they have targeting the power grid to attack [33].

6) In April 2009, Wall Street Journal quoted the saying of an unnamed national security official. He said that cyber spies in some countries had came into contact with U.S. power grid and installed malicious software tool used to shut down certain services. They also expressed the concern that a malicious hacker may attack during a crisis or war in the future [33], although this intrusion hadn't disrupt the normal operation of the power grid.

7) The Bushehr nuclear power plant in Iran was attacked by the computer worm Stuxnet on October 26, 2010. This worm invaded into the internal of the nuclear plant via USB device and destroyed the centrifuge in nuclear facilities. Meanwhile, the worm used fake data to deceive the operator through replay mode. Thus the virus invasion was undetectable to the operators. The virus is specific to Simatic WinCC SCADA system produced by Siemens company, which is used as industrial control systems in many critical infrastructures in China. Due to

the powerful function of Stuxnet virus, the team behind this virus must have superb professional technical staff and strong financial backing. The United States and Israel admitted that they developed the virus jointly soon [34].

A brief analysis of the actual events of cyber attacks mentioned above in respect of threat sources, vulnerabilities and assaulting modes is available according to the reports, though the relevant information is limited.

4.2. Threat Sources Analysis

From the perspective of threat source, the instances above can be analyzed as follows. Threat of instance 1 is derived from the worm. Instance 2 and 6 are associated with military action. Instance 3, 4 and 5 are typical hacker attack. Instance 7 is relatively complex. Due to its powerful destructive capability, stuxnet is not simple computer viruses and closely related to the national military behavior. Instances show that among the threat sources of cyber attacks, hacker, viruses and military action are the most typical. For in-depth analysis, there are many inherent relationships between these three threat sources. And these relations can't be clearly grasped from the current public information.

4.3. Assaulting Mode Analysis

After the text edit has been completed, the paper is ready for the template. Duplicate the template file by using the Save As command, and use the naming convention prescribed by your journal for the name of your paper. In this newly created file, highlight all of the contents and import your prepared text file. You are now ready to style your paper.

From the perspective of assaulting mode, instance 2, 5 and 7 are more likely replay attack. And instance 2 and 5 are possibly middle attack. Instance 1 and 6 are typically denial service attacks. The assaulting mode of instance 3 and 4 are not clear, and there exist multifold possibility.

According to the occurrence mechanism of the attacks, combined with instance analysis, qualitative comparisons are done according to the implementation difficulty and the severity of consequences (shown in **Figure 1**).

1) Denial service attack is easy to conduct as its various means and no need for the attacker having a deep understanding of the power system. Judging from the consequences, the influence of denial service attack is relatively small because it can't directly operate key equipments despite its huge influence on monitoring process.

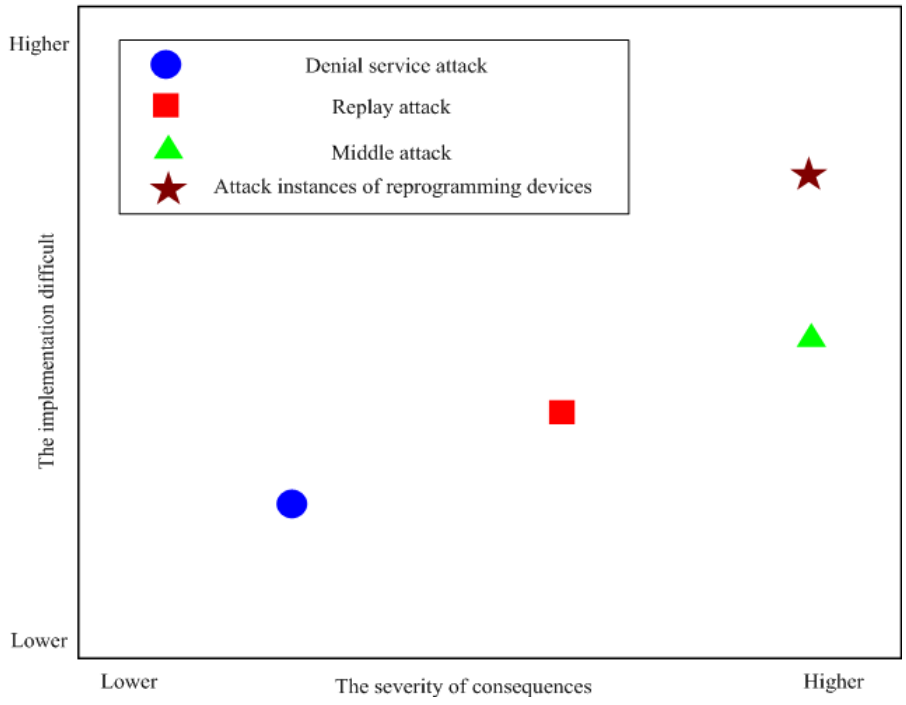

Figure 1. The comparison of impact and difficulty among the four cyber attack ways.

2) Replay attack and middle attack have much in common. And their essence is to achieve the purpose of maliciously operating critical equipment through attacker deceiving the recipient of information by certain means. But the difference between the two is that the replay attack has simpler means, and the goals able to achieve is less.

3) Attack instances of reprogramming devices haven't been found by far. But the occurrence of this kind of attack is possible in the future. Once succeed, the impact will be huge.

5. Conclusion

In summary, main reasons of the impact on power infrastructure caused by cyber attack are analyzed in respect of consequences and threats in this paper. The dependence of electric power infrastructure on information infrastructure determines the seriousness of the consequences of cyber attack. The main threats are diverse. The seriousness of the consequences improves the profit of cyber attacks, enhancing the motivation of attacks. Combined with the main assaulting mode of cyber attacks and currently reported attacks events, the impact of cyber attack on electric power infrastructure will gradually increase from the number and extent.

References

[1] Cleveland, F. (2006) IEC TC57 Security Standards for the power system's Information Infrastructure—Beyond Simple Encryption. *IEEE PES TD* 2005/2006, 21-24 May 2006, 1079-1087.

[2] Lin, C., Wang, Y. and Li, Q.L. (2005) Stochastic Modeling and Evaluation for Network Security. *Chinese Journal of Computers*, **28**, 1943-1956.

[3] Niu, P.C., Kang, J.T., Li, A.W. and Li, L. (2010) New Operation Form of Power Network Started by Smart Grid. *Power System Protection and Control*, **38**, 240-244.

[4] Li, W.W., You, W.X. and Wang, X.P. (2011) Survey of Cyber Security Research in Power System. *Power System Protection and Control*, **39**, 140-147.

[5] Watts, D. (2003) Security & Vulnerability in Electric Power Systems. *IEEE* 35*th North American Power Symposium Conference*, Rolla Missouri USA, 20-21-19 October 2003, 559-566.

[6] Lewis, J.A. (2011) The Electrical Grid as a Target for Cyber Attack. http://csis.org/files/publication/100322_ElectricalGridAsATargetforCyberAttack.pdf

[7] Kelic, A., Warren, D.E. and Philips, L.R. (2011) Cyber and Physical Infrastructure Interdependence. http://prod.sandia.gov/techlib/access-control.cgi/2008/086192.pdf

[8] Anderson, R.S. (2011) Cyber Security and Resilient Systems. http://www.inl.gov/technicalpublications/Documents/4311316.pdf

[9] Department of Homeland Security Office of Cyber Security and Communications National Cyber Security Division (2011) National Cyber Exercise: Cyber Storm. http://cryptome.org/cyberstorm.pdf

[10] China News Network (2011) Iranian Officials Have Accused the USA and Israel Manufacture of Computer Viruses Destroy Iranian Nuclear Facilities. http://www.chinanews.com/gj/2011/04-17/2977981.shtml

[11] Headquarters Department of the Army Washington, DC (2011) Infrastructure Risk Management (Army). http://www.apd.army.mil/pdffiles/r525_26.pdf

[12] State Electricity Regulatory Commission (2004) Power Monitoring System Security Requirements. Beijing.

[13] Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001) Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. *IEEE Control Systems*, **21**, 11-25. http://dx.doi.org/10.1109/37.969131

[14] Liu, J.F., Chen, C.P. and Luo, J. (2004) Design and Application of Information's Security and Protection in Power Supervision and Control Automatic System. *Relay*, **32**, 33-35.

[15] Wu, G.W. (2007) Information Disposal and Network Security Analysis in Digital Substation. *Relay*, **35**, 18-22.

[16] Du, G.H. and Wang, Z.F. (2010) Design and Research on Power Network Dispatching Integration of Smart Grid. *Power System Protection and Control*, **38**, 127-131.

[17] Stamp, J. and Mcintyre, A. (2009) Reliability Impacts from Cyber Attack on Electric Power Systems. *The* 2009 *Power Systems Conference and Exposition*, Seattle, 15-18 March 2009, 1-8.

[18] Tatum, M. (2011) What Is a Cyber attack? http://www.wisegeek.com/what-is-a-cyberattack.htm

[19] Substations Committee of the IEEE Power Engineering Society (2008) IEEE Guide for Electric Power Substation Physical and Electronic Security, IEEE Std 1402-2000(R2008). USA.

[20] IEC TS 62351-1 (2007) Power Systems Management and Associated Information Exchange—Data and Communications Security Part I: Communication Network and System Security—Introduction to Security Issues. Geneva.

[21] Li, J. (2011) Academician Disclose the Cyber Attack Is Very Serious in China. http://society.people.com.cn/GB/1062/9343749.html

[22] Mu, L.H., Zhu, G.F. and Zhu, J.R. (2010) Design of Intelligent Terminal Based on Smart Grid. *Power System Protection and Control*, **38**, 53-56.

[23] Han, Y.J., Zhao, N.Q. and Liu, Y.C. (2005) Destructive Mechanism of Blackout Bomb and Its Defending Measures *Ordnance Material Science and Engineering*, **28**, 57-60.

[24] Zhang, Y.Q. (2011) Network Attack and Defense Technology. Tsinghua University Press, Beijing, 59-65.

[25] Baigent, D., Adamiak, M. and Mackiewicz, R. (2011) IEC61850 Communication Networks and Systems in Substations: An Overview for Users. http://www.sisconet.com

[26] Negrete-Pincetic, M., Yoshida, F. and Gross, G. (2009) Towards Quantifying the Impacts of Cyber Attacks in the Competitive Electricity Market Environment. *Bucharest Power Tech Conference*, Romania, 28 June-2 July 2009, 105-111.

[27] Liu, N., Zhang, J.H. and Duan, B. (2009) Design of Security Mechanism for Substation Remote Configuration Based on XML Security. *Electric Power Automation Equipment*, **29**, 113-117.

[28] Taylor, C., Krings, A. and Foss, J.A. (2011) Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.80.8323&rep=rep1&type=pdf

[29] Hu, Y., Xie, X.R., Han, Y.D., *et al*. (2005) A Survey to Design Method of Security Architecture for Power Information Systems. *Power System Technology*, **29**, 35-39.

[30] Greenberg, A. (2011) Congress Alarmed at Cyber-Vulnerability of Power Grid. http://www.forbes.com/2008/05/22/cyberwar-breach-government- tech-security_cx_ag_0521cyber.html

[31] Meserve, J. (2011) Staged Cyber Attack Reveals Vulnerability in Power Grid. http://articles.cnn.com/2007-09-26/us/power.at.risk_1_generator-cyber-attack-electric-infrastructure?_s=PM:US

[32] Poulsen, K. (2011) Report: Cyber Attacks Caused Power Outages in Brazil. http://www.wired.com/threatlevel/2009/11/brazil/

[33] Oman, P., Schweitzer, E. and Roberts, J. (2011) Protecting the Grid from Cyber Attack Part I: Recognizing Our Vulnerabilities. http://www.elp.com/index/display/article-display/130136/articles/utility-automation-engineering-td/volume-6/issue-7/features/protecting-the-grid-from-cyber-attack-part-i-recognizing-our-vulnerabilities.html

[34] Wikipedia (2011) Stuxnet. http://en.wikipedia.org/wiki/Stuxnet