Essentials of Passive Defense in Electric Power Systems

Mohammad Adelpour, and Hassan Ghasemi, *Senior Member*, *IEEE*
School of Electrical and Computer Engineering
University of Tehran
Tehran, Iran
Emails: m.adelpour@ut.ac.ir , h.ghasemi@ut.ac.ir

***Abstract*— Critical infrastructures especially electric power systems play a key role in sustainable development of modern societies; therefore, power systems security has attracted significant attention in recent years. Concerns about malicious attacks on electric power grids, e.g. terrorist attacks, have manifested the necessity of passive defense implementation to reduce the likelihood of successful attacks and to minimize the damages and negative consequences. To optimally allocate passive defense resources, familiarity with issues related to power system security aspects, vulnerabilities, interaction with other infrastructures, crisis management stages and time scale, beneficial and adverse technologies, and hardening optimization methodologies is needed. This paper provides an extensive overview of passive defense essentials in electric power systems.**

Keywords- Critical infrastructures; defense plan; infrastructures interdependency; passive defense; power system security.

I. INTRODUCTION

High quality of life in today's modern societies is indebted to continuous operation of infrastructures. Since sustainable economic and social developments are impossible in case of infrastructures vulnerability, security of infrastructures including oil, gas, water and wastewater, electricity, telecommunication, transportation, banking and finance, and emergency services has attracted significant attention in recent years [1]-[20]. Many countries have developed plans to protect their national critical infrastructures; e.g., European Programme for Critical Infrastructure Protection (EPCIP) and National Infrastructure Protection Plan (NIPP) in the US [3]. Among different infrastructures, electricity has high importance [1], [2], [7]-[15], and sometimes is considered as the fundamental infrastructure [7].

Concerns about malicious attacks on electric power system infrastructures, like terrorist and military attacks, have increased in recent years [1]-[13]. To protect power systems, beside guards or army conscripts, implementation of passive defense (i.e., taking measures to reduce the likelihood of successful attacks and to minimize the damages and negative consequences) is necessary [9], [13]. For example, hardening transmission tower legs using concrete sheaths is a passive defense technique [13]. To optimally allocate the available passive defense resources, it is necessary to be familiar with power system security aspects, vulnerabilities, interaction with other infrastructures, crisis management process, impact of technologies on power system security, and optimal hardening methodologies.

This paper aims at providing an extensive overview of passive defense essentials in electric power systems. Section 2 discusses different aspects of power system security. In Section 3, infrastructures interdependency and power system interaction with other infrastructures are discussed. In Section 4, intentional damages to power systems are described. Section 5 discusses the timescale of crisis management in power systems. Section 6 is about the impact of technology (adverse and beneficial) on power system security. Optimal hardening against physical antagonistic attacks on power systems are discussed in Section 7. Finally, Section 8 concludes the paper.

II. ELECTRIC POWER SYSTEM SECURITY

Electric power systems face variety of threats including natural hazards, component failures, Human errors and intentional damages [8], [10]. Security of power system can be categorized into: operational security, robustness to physical damages, and cyber security (Fig. 1). From operational point of view, which is a well-known topic to electrical power engineers, transient, dynamic and voltage stability, contingencies, coordination of areas, reliability and other ordinary concepts associated with power system operation should be considered [7], [10]. Today's power systems have become very complex, e.g., "The North American electric power system has been called the most complex machine ever built" [10]. Complexity of power system causes operation difficulties as well as vulnerability [10]. Skill and proficiency of system operators is another aspect of operational security; since in response to critical situations, operators may make serious mistakes [7]. Natural hazards (e.g., earthquakes, hurricanes, tornados, thunderstorms, storms, etc) can cause physical damages to power systems [13]. New vulnerabilities have been emerged by modern Information Technology (IT) [14]. Today's power systems are remotely controlled by Supervisory Control And Data Acquisition (SCADA) systems that rely on internet and telecommunication [4]. Furthermore, internet is necessary for electricity market functions [8]. Although these technologies increase the system efficiency,

978-1-4673-1148-9/12/$31.00 ©2012 IEEE

they bring external threat and intensify the complexity [8]. Nowadays, we face complex "cyber-physical" power systems [21]. Therefore, both physical and cyber damages to power system can be caused by malicious activities which will be discussed in Section 4.

However, what is more important is the vulnerability of society to electricity interruption not the vulnerability of power system by itself [15]. For example, societal vulnerability to electricity disruption in a power system feeding a cold area relying on electrical heaters is much more than an area with moderate climate. Infrastructures like electric power systems that have social aspects beside technical aspects are called "socio-technical systems" [1].

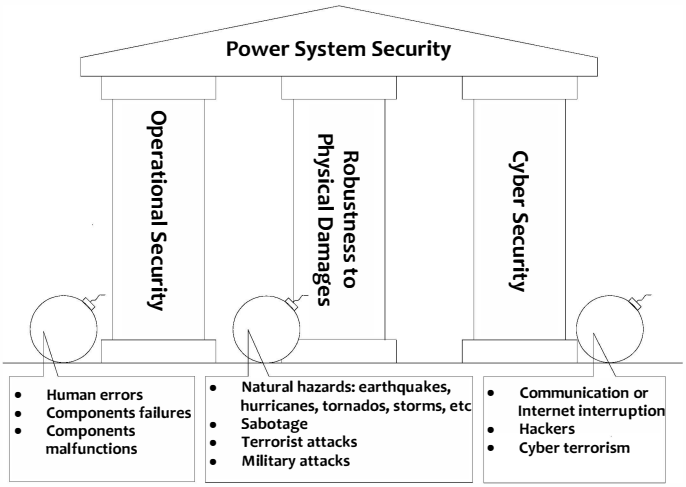

Figure 1. Power system security structure and threats

III. INFRASTRUCTURES INTERDEPENDENCY

In modern societies, infrastructures are tightly interdependent and form a large complex ''systems of systems'' [1]-[8], [16]. Two kinds of interdependency among infrastructures can be defined: spatial interdependency and functional interdependency [16]. When infrastructure facilities are closely located and are independent in operation, they are spatially interdependent [16], e.g., water pipes and electricity cables may pass the same service tunnel in urban areas [6]. Functional interdependency refers to necessity of one infrastructure for operation of another one, e.g., water treatment plants need electricity to operate the pumps [16]. The disadvantage of interdependency is vulnerability enlargement [2], [16].

Electric power infrastructure is thought to be the most critical infrastructure since other infrastructures heavily rely on it [1], [2], [7]-[15]. As an example, the power system blackout in southern Sweden and eastern Denmark in 2003 which affected 5 million people clearly illustrates other infrastructures dependency on power systems. During the incident, cell-phone system stopped working, communication system of police faced some problems, the bridge between Sweden and Denmark was closed because of failure in monitoring system and led to sever traffic problems. Railway operation in some parts of Sweden and Denmark stopped. Copenhagen air port's halt of activity created a serious air traffic problem [1].

Data and back-ups corruption due to short electricity interruption shut Vancouver Stock Exchange down for a day [17], as an example showing the effect of power system on economy. Hospitals which provide important emergency services extremely rely on electricity. Although they have emergency power systems, these systems have limited capacity and they may face some technical problems when they are needed [1], [13]. Infrastructures interdependency shows the paramount importance of power systems security.

On the other hand, Power systems depend on other infrastructures as well and may stop working due to problems in other infrastructures [16]. As was mentioned earlier, power systems intensely rely on computers, communication and internet, e.g., failure of some software systems were one of the main causes that led to blackout in the US and Canada in 2003 [16]. Since many power plants rely on natural gas and oil, security of gas/oil pipelines also has a remarkable effect on power systems [5], [10], [19].

IV. FOCUS ON INTENTIONAL DAMAGES

Intentional damages to power system can be caused by: vandalism, sabotage, terrorism and military attack [13]. Vandals, like hunters who shoot at insulator of overhead lines, are unlikely to cause notable damages [13]. Some intentional actions initiate over labor disputes. Commonly in this kind of sabotage, the attacker does not aim at causing a widespread blackout and just wants to harm the utility.

Threat of terrorist attack against infrastructures had been identified and remarked prior to incident of September 11, 2001 (e.g., [13], [18]); However, this event manifested the risk of terrorist attack against infrastructures [1]-[12]. Increase in purchasing terrorism insurance is good evidence that illustrates concerns of electric power industry about terrorism [11]. Several countries have faced malicious attacks on their electric power grids, including: Brazil, Chile, Colombia, France, Russia, Spain, Sweden and Turkey [11]. Among these countries, Colombia is a clear example for terrorist attack against electric power system. Colombia's power grid has experienced 200 attacks per year during last 11 years; most of them aimed at transmission infrastructure and have caused 2,740 towers to be destroyed [22]. Colombia is suffering from armed conflicts and malicious activities are made by insurgent groups [22], [11].

In case of war, defending electric power system infrastructure is vital. Power systems are important for fates of wars; e.g., destruction of Germany's electric power system is one of the important causes of World War II ending. ''The war would have finished two years sooner if you (the Allies) had concentrated on the bombing of our power plants earlier" this is what German officers said after the war [13]. Countries like Serbia (during the Kosovo war in 1999) and Iraq (during the first Gulf war in 1991) have faced military attacks against their power networks [23].

Power system is also exposed to threat of hackers and cyber terrorism [4]. For example, injection of false

information by means of measurement manipulation is a kind of cyber attack against power system which will lead to false security-constrained economic dispatch and can cause the power system to operate uneconomically or even unsecure [24]. Due to existing motivation in developing and using smart grids worldwide, the cyber security problems of smart grids is important to address [25]. Some think cyber attacks are harder than physical attacks to perform [26]; however, it should be noticed that cyberspace has no border and cyber attacks can be implemented from anywhere around the world [4].

V. Time Scale of Crisis Management

Form timing perspective, crisis management contains three phases: before, during and after an incident (see Fig. 2). This section discusses the actions which should be done in each stage.

A. Before an Incident

First step is vulnerability analysis and risk assessment that lead to critical assets identification and ranking [9]. Vulnerability analysis can be viewed from three different perspectives: global vulnerability, critical components vulnerability, and geographical vulnerability [1]. Global vulnerability gives a view of vulnerability level of system as a whole to different types and magnitudes of strain. For example, power system performance assessment when a fraction of nodes are lost is a global vulnerability study. A wide range of strain magnitude from small to very sever ones is considered in global vulnerability analysis [1]. Network theory can be used as a tool for large-scale infrastructures analysis [1], [27], [28]. From network theory perspective, some power system technical limitations are not taken into account. For instance, the authors in [28] have modeled a power grid as a network of nodes and edge assuming that a generator can feed a load if a path exists between them and ignoring the capacity of lines and other system constraints.

Critical components vulnerability analysis aims at determining crucial components that their failure will cause significant damages [1]. Quantitative measures are needed for vulnerability analysis and components ranking [29]. Reference [30] proposes a model for quantifying vulnerability of infrastructures. Some vulnerability indices for power system have been proposed as well, e.g., [29], [31]. Information and data importance assessment and ranking should be done as well in order to determine the most critical ones [26].

In geographical vulnerability assessment that focuses on location of components, natural hazards are considered. Recognition of critical locations that are expected to be targets of destructive attacks (e.g., bombing) is another aspect of geographical vulnerability analysis [1]. For identification of critical locations, spatial interdependency of infrastructures should be taken into account as well [32].

For quantitative risk analysis (QRA) these three questions should be answered [33]:

- What can happen?
- How likely is it?
- What will be the consequences?

In order to answer the first question, different possible risk scenarios should be considered. Since infrastructures like power systems are large-scale complex systems, many different risk scenarios can be defined. Thus, scenario reduction methodologies will be useful [4]. Determination of component failure probability is common and is used for studying the system reliability; however, it is not easy to estimate the likelihood of malicious attacks to answer the second question [1], [34]. Nonetheless, record of previous incidents has helped estimate probability of malicious attacks [11]. According to a study based on historical data related to attacks against grid components, in 60% of incidents, transmission lines and towers were aimed. Among different components of power networks, power plants are thought to be the most difficult to attack [11]. The location and accessibility of component directly affect their likelihood to be attacked, e.g., a substation in urban area that is under local police surveillance is much more unlikely to be attacked than a substation in suburban area [12]. Following an attack, the probability of its success is important and should be considered. Some approaches to deal with uncertainty in determining probability of attack success are discussed in [12]. Technical analyses are very useful in studying probability of attack success, e.g., reference [35] derives probability of a substation failure as a function of distance from explosion by modeling and simulation. In order to answer the third question, the consequences of each risk scenario should be analyzed. Analyzing previous incident is useful to estimate what consequences to expect [11]. Negative consequences of an interruption depend on magnitude, duration and time of the event [17].

Next step is determination of possible countermeasures [9] and preparation of an appropriate defense plan. Defense plan should protect the system against a wide spectrum of threats [8]. However, it is not possible to make a system fully invulnerable and a rational level of risk is acceptable. So, a trade of between risk and cost should be done [3]. Mitigation and prevention activities can be done to reduce likelihood of damages. Moreover, preparedness activities can be done to minimize the consequences, to have appropriate and timely response, as well as fast recovery [1]. The available resources must be allocated optimally between different possible actions. Preparation of Security guidelines (e.g., [36]) and threat response plan for different levels of alert (e.g., [9]) are necessary. Also, security concepts should be considered in system expansion and planning [5], [37].

Necessary activities in this phase (before an incident) can be summarized as below:

- Risk and vulnerability assessment
- Preparation of an appropriate and optimal defense plan including: guidelines, prevention, mitigation, and preparedness.

B. During an Incident

In case of an emergency, the system should respond to crisis properly and timely; thus, this stage is also named response phase [1], [38]. It is vital to avoid cascading failures following each disturbance. Cascading failures are very likely to cause a blackout [39]; e.g., reference [40] explains how

cascading failures led the Italian power network to a general blackout on September 28, 2003. Protection system malfunction increases the chance of encountering cascading failures [22], [27]. A strong real-time protection and control system is needed to make critical decisions in case of emergency [8].

Making the right decision at the right moment is vital, e.g., earlier implementation of load shedding would have avoided the Italian blackout in 2003 [40]. Flexible islanding (i.e., break the system to separate islands that can operate individually) is an approach for protection of the system in case of emergency [7], [8], [41].

Control centralization has brought some vulnerability to power system, since central control center can be attacked [2]. Availability of a back up control system is another scheme to deal with risk of losing a control center. Back up control system operates continuously and in parallel to the main control system; and in case of contingency, it would take over on the whole control of the system [22].

C. *After an Incident*

After an emergency, the damaged system should be recovered; so, this phase is also called recovery stage [1], [38]. Duration of an interruption determines the negative consequences, i.e., the faster system recovery means the less loss and cost [17]. Availability of spare components will lead to a faster system restoration, e.g., transporting and repairing large transformers are difficult and take lots of time; therefore, keeping spare transformers near the operating ones (in a safe place) is helpful [13], [11].

Learning from historical events is important to get useful feedback to improve the defense plan, guidelines and identification of deficiencies [1].

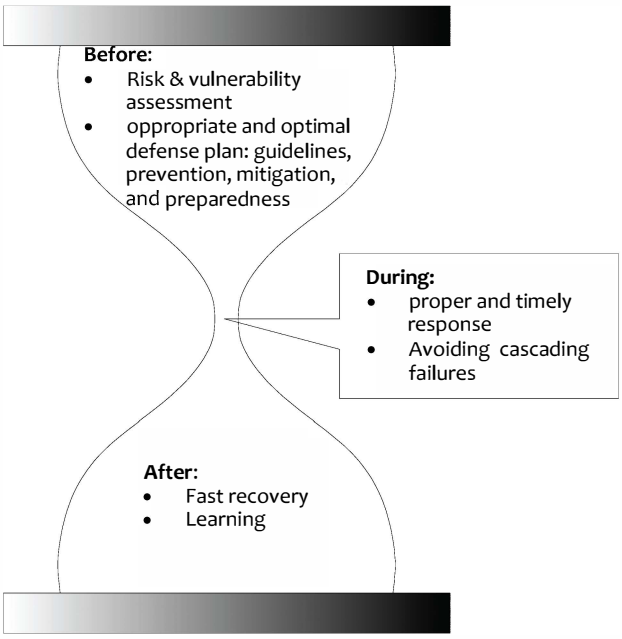

Figure 2. Crisis management time scale

VI. Role of Technology in Power System Security

Some modern technologies like IT make the power system more complex and vulnerable; however, technology can help avoid system damages and faster recovery following an incident. Using less vulnerable technologies, like underground cables instead of overhead lines, decreases the probability of successful antagonistic actions. However, underground cables need expensive and difficult maintenance. Moreover, if they fail or are attacked, they would lead to longer outages [13], [17]. Research is being conducted to develop technologies in order to protect infrastructures [42]. Below two technologies are discussed that can be used to harden and achieve faster system recovery.

Insulated Bus Pipe (IBP): Exposed conductors and bus bars make outdoor air insulated substations vulnerable to vandalism and terrorist attacks. Using insulated conductors instead of exposed ones is a way of substation hardening. IBP is a commercially available product that can be used to replace exposed conductors [43].

Emergency pylons: As was mentioned before, power transmission lines are more likely to be attacked. Fast restoration of damaged lines is vital for decreasing costs due to power outage. Emergency pylons are easy to transport and handle, need no foundation, proper for any voltage level and compatible with different structures such as suspension, tension or angle, and have been successful experience in fast system restoration [22].

On the other hand, technology can be used to damage infrastructures as well; e.g., graphite bombs are clear evidence. These bombs release long, thin, and conductive graphite filaments into the air, which land on power lines or transformers and cause failures. Graphite bombs caused 70% of Serbia to be in darkness during the Kosovo war in 1999 [23].

VII. Optimal Hardening against Physical Antagonistic Attacks: Studies and Methodologies

The two important differences between malicious attacks and other threats are hostility and smartness. Among different kinds of threats, it is more difficult to deal with sabotage and terrorist attacks; because these actions are secretive and antagonistic [8], [38]. Malicious attacks are selective, i.e., the attacker selects the target and the time of attack [38]. Moreover, they can be coordinated [13] e.g., 11 attacks to the power network of Colombia occurred in a single night in 2002 [22]. Terrorists are often intelligent and they usually gather information before a strike [44]. In order to analyze natural hazards, statistical methods are used and component failures are analyzed by means of stochastic theory. But these methods are not suitable to study malicious attacks [45]. Since malicious attacks differ from other threats, their modeling and study need different techniques. Interaction between the attacker and defender is another aspect of malicious attacks [38], [45].

Attack modeling is the first step to study hardening against malicious attacks. Different attack models have been proposed. From knowledge of attacker about the system and

defender strategies viewpoint, attackers are classified into four categories [38], [44]-[50]:

- Uninformed
- Partly informed
- Fully informed
- Misinformed

Uninformed attacker chooses the target randomly [38], [44], but an informed one most likely tries to maximize the negative consequences [38], [44]-[49]. Some of the proposed attacker objectives are as below:

- Maximal load shed attack [38]
- Maximum capacity based attack [47]
- Maximum flow based attack [47], [51]
- Maximum cost attack [44]-[49]

Resources can be allocated either to reinforce physical hardening such as barriers and fortification [38], raise generation or lines capacity, preparation of spare transformers [47] or recovery [38]. Defending a component decreases the probability of a successful attack against it; and the allocation of resources for recovery leads to a shorter interruption. In order to optimize the allocation of resources, probability of attack and recovery duration should be modeled as functions of allocated budget [38], [44]. Although in many studies the negative consequences of attacks are modeled as amount of load shed or cost [38], [44]-[49], modeling of some social and psychological impacts as 'dollar cost' is not acceptable and a risk assessment based on multiple criteria is needed [34].

In early studies, only the most damaging scenario was studied, and it was thought that defending the equipments whit the highest loss impact is optimal hardening plan [48], [49], [51]. But it should be noticed that the maximization of consequences is not the only possible purpose of attackers. They may attack the power system as a symbolic demonstration or to obtain a political, economical, etc goal. To spread fear, it is sufficient to choose a damaging enough scenario [38]. Thus, many different scenarios are possible to be chosen by the attacker. Unfortunately, for each attack strategy, a different defense strategy is optimal and a global optimal strategy does not exist [44]. Moreover, an attacker who is fully informed about the system and the hardening strategy adapts the attack plan to the condition dynamically [45]. Different methodologies have been used for modeling and solving the optimization problem including: integer programming [47], [52], genetic algorithm [46], and game theory. Game theory is very capable for modeling the interaction between attacker and defender [38], [44], [45] and leads to more reliable defending strategies [44]. It is believed that modeling malicious attacks against power systems is in the beginning of the way [45].

VIII. CONCLUSION

Since electric power systems play a key role in sustainable development of societies and extremely affect other infrastructures, they are attractive targets to terrorist activities and military attacks. Intentional attacks to power systems, because of their antagonistic nature, are more difficult than other threats to deal with. These attacks can be physical strikes or offensive cyber actions. Implementation of passive defense is necessary to reduce the likelihood of successful attacks and to minimize the damages and negative consequences. Risk and vulnerability assessment is necessary to prepare appropriate defense plans including: guidelines, prevention, mitigation and preparedness. Power system must respond timely and properly in case of encountering a disturbance and cascading failures should be avoided. Fast recovery of power system after an incident is vital for reduction of negative consequences. Security concepts should also be considered in power system planning and expansion. Infrastructures interdependency must be considered; especially, attention to security of gas/oil infrastructures is essential in power system passive defense planning. Beneficial technologies should be identified, developed and used in passive defense implementation. Adverse technologies which may be used to damage power system should be taken into account as well. Among hardening optimization methodologies, game theory is highly capable to model interactions between attackers and defenders. Modeling malicious attacks and optimal hardening against them are ongoing research subjects.

REFERENCES

[1] J. Johansson, "Risk and vulnerability analysis of interdependent technical infrastructures," Ph.D. dissertation, Lund Univ., Dep. Measurement Technology and Industrial Electrical Eng., 2010.

[2] M. Amin, "Toward secure and resilient interdependent infrastructures," Journal of Infrastructure Systems, pp. 67–75, Sep. 2002.

[3] J. M. Yusta, G. J. Correa, and R. Lacal-Arantegui, "Methodologies and applications for critical infrastructure protection: State-of-the-art," Energy Policy, vol. 39, no. 10, pp. 6100–6119, Oct. 2011.

[4] Y. Y. Haimes and T. Longstaff, "The role of risk analysis in the protection of critical infrastructures against terrorism," Risk Analysis, vol. 22, no. 3, pp. 439-444, 2002.

[5] H. Zerriffi, "Electric power systems under stress: an evaluation of centralized versus distributed system architectures," Ph.D. dissertation, Carnegie Mellon Univ., Carnegie Institute of Technology, 2004.

[6] G. E. Apostolakis and D. M. Lemon, "A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism," Risk Analysis, vol. 25, no. 2, pp. 361-376, Apr. 2005.

[7] M. Amin, "Security challenges for the electricity infrastructure," Computer, vol. 35, no. 4, pp. 8-10, Apr. 2002.

[8] H. Li, G. W. Rosenwald, J. Jung, and C.-C. Liu, "Strategic power infrastructure defense," in Proceedings of the IEEE, vol. 93, May 2005, pp. 918–933.

[9] M. R. Gent and L. P. Costantini, "Reflections on security," IEEE Power & Energy Magazine, vol. 1, no. 1, pp. 46-52, Jan./Feb. 2003.

[10] M. Amin, "Energy infrastructure defense systems," Proceedings of the IEEE, vol. 93, no. 5, pp. 861-875, May 2005.

[11] R. Zimmerman, C. Restrepo, N. Dooskin, R. Hartwell, J. Miller, and W. Remington, "Electricity case: main report – risk, consequences, and economic accounting," CREATE, Tech. Rep. May 2005.

[12] B. J. Garrick, J. E. Hall, M. Kilger, J. C. McDonald, T. O'Toole, P. S. Probst, E. R. Parker, R. Rosenthal, A. W. Trivelpiece, L. A. V. Arsdale, and E. L. Zebroski, "Confronting the risks of terrorism: making the right decisions," Reliability Engineering and System Safety, vol. 86, no. 2, pp. 129–176, Nov. 2004.

[13] "Physical vulnerability of electric systems to natural disasters and sabotage," Office of Technology Assessment, U.S. Congress, Washington, DC, Tech. Rep OTA-E-453, June 1990.

[14] S. S. Oren, "Risk management vs. risk avoidance in power systems," in IEEE Power Engineering Society General Meeting, June 2006.
[15] J. Johansson, H. Jonsson, and H. Johansson, "Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions," Int. J. Emergency Management, vol. 4, no. 1, pp. 4-17, 2007.
[16] R. Zimmerman, "Decision-making and the Vulnerability of Interdependent Critical infrastructure," in IEEE Int. Conf. Systems, Man and Cybernetics, vol. 5, 2004, pp. 4059-4063.
[17] M. Greenberg, "Impact to New Jersey's economy of the Loss of electric power in New Jersey's urban industrial corridor," CREATE, Tech. Rep. 2005.
[18] L. Leffler, "The NERC program for the electricity sector critical infrastructure protection," in IEEE Power Engineering Society Winter Meeting, vol. 1, 2001, pp. 95-97.
[19] M. Shahidehpour, Y. Fu, and T. Wiedman, "Impact of natural gas infrastructure on electric power systems," in Proceedings of the IEEE, May 2005, pp. 1042 - 1056.
[20] Z. Skolicki, M. M. Wadda, M. H. Houck, and T. Arciszewski, "Reduction of physical threats to water distribution systems," Journal of Water Resources Planning and Management, vol. 132, no. 4, pp. 211-217, July/Aug. 2006.
[21] B. McMillin, "Complexities of information security in cyber-physical power systems," in Power Systems Conference and Exposition, Seattle, Mar. 2009.
[22] H. Pablo and M. E. Ruiz, "Against all odds," IEEE power & energy magazine, vol. 9, no. 2, pp. 59-66, Mar./Apr. 2011.
[23] W. Fang, F. Shunshan, W. Wenxuan, and L. Fuwang, "Analysis of action mechanism of graphite bombs and reaction method of power system," in Int. Conf. Power System Technology, 2010.
[24] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution Attacks in power systems," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 382-390, June 2011.
[25] F. Cohen, "The smarter grid," IEEE Security & Privacy, vol. 8, no. 1, pp. 60-63, Jan./Feb. 2010.
[26] E. Bompard, R. Napoli, and F. Xue, "Assessment of information impacts in power systems security against malicious attacks in a general framework," Reliability Engineering and System Safety, no. 94, pp. 1087-1094, 2009.
[27] G. Chena, Z. Y. Dong, D. J. Hill, G. H. Zhang, and K. Q. Hua, "Attack structural vulnerability of power grids: A hybrid approach based on complex networks," Physica A, no. 389, pp. 595–603, 2010.
[28] I. Albert, G. L. Nakarado R. Albert, "Structural vulnerability of the North American power grid," Physical Review E, vol. 69, no. 2, 2004.
[29] M. Kim, M. A. El-Sharkawi, and R. J. Marks, "Vulnerability indices for power systems," in 13th Int. Conf. Intelligent Systems Application to Power Systems, 2005, pp. 335 - 341.
[30] B. C. Ezell, "Infrastructure vulnerability assessment model (I-VAM)," Risk Analysis, vol. 27, no. 3, pp. 571–583, 2007.
[31] M. Anji and Y. Jiaxi and G. Zhizhong, "Electric power grid structural vulnerability assessment," in IEEE Power Engineering Society General, 2006.
[32] S. A. Patterson and G. E. Apostolakis, "Identification of critical locations across multiple infrastructures for terrorist actions," Reliability Engineering and System Safety, vol. 92, pp. 1183-1203, 2007.
[33] S. Kaplan and B. J. Garrick, "On the quantitative definition of risk," Risk Analysis, vol. 1, no. 1, pp. 11–27, 1989.
[34] A. M. Koonce, G. E. Apostolakis, and B. K. Cook, "Bulk power risk analysis: Ranking infrastructure elements according to their risk significance," Electrical Power and Energy Systems, vol. 30, no. 3, pp. 169-183, March 2008.
[35] L. G. Roybal, R. F. Jeffers, K. E. McGillivary, T. D. Paul, and R. Jacobson, "Modeling and simulating blast effects on electric substations," in IEEE conf. Technologies for Homeland Security, 2009, pp. 351–357.
[36] Security guidelines for the electricity Sector: physical security, 2007, North American Electric Reliability Corporation.
[37] M. Carrin, J. M. Arroyo, and N. Alguacil, "Vulnerability-constrained transmission expansion planning: a stochastic programming approach," IEEE Trans. Power Systems, vol. 22, no. 4, pp. 1436–1445, Nov. 2007.
[38] A. J. Holmgren, E. Jenelius, and J. Westin, "Evaluating strategies for defending electric power networks against antagonistic attacks," IEEE Trans. Power Systems, vol. 22, no. 1, pp. 76-84, Feb. 2007.
[39] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, "Critical points and transitions in an electric power transmission model for cascading failure blackouts," CHAOS, vol. 12, no. 4, pp. 985-994, Dec. 2002.
[40] S. Corsi and C. Sabelli, "General blackout in Italy Sunday September 28, 2003, h. 03:28:00," in IEEE Power Engineering Society General Meeting, 2004, pp. 1691 - 1702.
[41] J. A. Hollman, J. R. Marti, J. Jatskevich, and K. D. Srivastava, "Dynamic islanding of critical infrastructures, a suitable strategy to survive and mitigate critical events," Int. J. Emergency Management, vol. 4, no. 1, pp. 45-58, 2007.
[42] C. Garcia, Y. Hernandez, D. Fernandez, M. A. Ferrer, C. M. Travieso, J. B. Alonso, and P. Henriquez, "HESPERIA: homeland security technologies for the security," in 41th IEEE Annual Int. Carnahan Conf. Security Technology, 2007, pp. 221-226.
[43] R. Worth, M. Islam, and C. Smith, "Insulated Bus Pipe (IBP) for power utility applications," in IEEE 11th Int. Conf. Transmission & Distribution Construction, Operation and Live-Line Maintenance, 2006.
[44] G. Chen, Z. Y. Dong, D. J. Hil, and Y. S. Xue, "Exploring reliable strategies for defending power systems against targeted Attacks," IEEE Trans. Power Systems, vol. 26, no. 3, pp. 1000-1009, Aug. 2011.
[45] E. Bompard, C. Gao, R. Napoli, A. Russo, M. Masera, and A. Stefanini, "Risk assessment of malicious attacks against power systems," IEEE Trans. Systems, Man, and Cybernetics, vol. 39, no. 5, pp. 1074-1085, Sep. 2009.
[46] G. Levitin, "Optimal defense strategy against intentional attacks," IEEE Trans. Power Systems, vol. 56, no. 1, pp. 148-157, Mar. 2007.
[47] N. Romero, N. Xu, L. K. Nozick, I. Dobson, and D. Jones, "Investment planning for electric power systems under terrorist threat", accepted to IEEE Trans. Power Systems.
[48] K. Wood, R. Baldick J. Salmeron, "Analysis of electric grid security under terrorist threat," IEEE Trans. Power Systems, vol. 19, no. 2, pp. 905-912, May 2004.
[49] Y. Yao, T. Edmunds, D. Papageorgiou, and R. Alvarez, "Trilevel optimization in power network defense," IEEE Trans. Systems, Man, and Cybernetics, vol. 37, no. 4, pp. 712-718, July 2007.
[50] H. Ben-Haim G. Levitin, "Importance of protections against intentional attacks," Reliability Engineering and System Safety, no. 93, pp. 639-646, 2008.
[51] V. M. Biera, E. R. Gratza, N. J. Haphuriwata, W. Maguaa, and K. R. Wierzbickib, "Methodology for identifying near-optimal interdiction strategies for a power transmission system," Reliability Engineering and System Safety, no. 92, pp. 1155–1161, 2007.
[52] A. L. Motto, J. M. Arroyo, and F. D. Galiana, "A mixed-integer lp procedure for the analysis of electric grid security under disruptive threat," IEEE Trans. Power Systems, vol. 20, no. 3, pp. 1357–1365, Aug. 2005.