Electrical Power and Energy Systems 50 (2013) 50–64

Contents lists available at SciVerse ScienceDirect

Electrical Power and Energy Systems

journal homepage: www.elsevier.com/locate/ijepes

Classification and trend analysis of threats origins to the security of power systems

Ettore Bompard [a], Tao Huang [b,c,*], Yingjun Wu [b], Mihai Cremenescu [d]

[a] Joint Research Center of the European Commission, Institute for Energy and Transport, Petten (NL)
[b] Dipartimento Energia, Politecnico di Torino, Torino 10129, Italy
[c] Key Laboratory of Control of Power Transmission and Transformation, Ministry of Education, Department of Electrical Engineering, Shanghai Jiao Tong University, Shanghai 200240, China
[d] Romanian Power Grid Company - TRANSELECTRICA S.A. Bucharest, 030236, Romania

ARTICLE INFO

Article history:
Received 4 September 2012
Received in revised form 21 January 2013
Accepted 15 February 2013
Available online 19 March 2013

Keywords:
Threats identification
Threats classification
Trend analysis
Power system security

ABSTRACT

This paper presents a framework to classify threats to power system secure operation. Threats have long been recognized; however, there lacks a categorical classification of them due to various individual perspectives from different organizations. The power system is evolving to a smart, super, and clean grid, accompanied by interior diversified and emerging threats. Furthermore, threats from exterior factors, intentional and non-intentional, conventional and new-born, to power systems have become more severe than ever before. Therefore, a distinct catalogue, description, and possible impact of these threats are proposed to meet the need of preventing power system from dangers. Using the proposed classification, a quantitative trend analysis of more than a hundred representative historic blackouts is performed to figure out the principal threats and the changing trend of threats over time.

1. Introduction

As a critical and fundamental infrastructure, power system's security problem is a global concern strongly associated with the social stability and economic development. Therefore, priorities have always been given by different authorities, organizations, and utilities at all levels. Once the power system is impacted by various threats which cause the system unsecure, for some extreme scenarios, the electric network might be split and large-scaled area may face blackout. As a consequence, it will generate numerous economic losses, in some situations, human lives and even national security will be in peril. Such results could be clearly observed in several more recent blackouts; for example, in the blackout of November 4, 2006 in Europe [1], a power imbalance in the Western part of the UCTE (Union for the Co-ordination of Transmission of Electricity) grid induced severe frequency deviation that caused splitting of the whole grid into three areas and an interruption of electricity supply to more than 15 million European households. Moreover, our lives in recent decades increasingly have relied on a high integration of different interdependent systems [2]. Electricity, as a main energy source to other infrastructures, stands in the center and is essential to the operation of all other systems. For instance, in the 2003 Northeast Blackout, water pressure was lost because pumps lacked power; all the trains running into and out of New York were shut down; cellular communication devices were disrupted; and cable television systems were disabled due to the loss of backup power [3].

For guaranteeing the security of power systems, threats to power system have long been recognized [4]. Threats causing blackouts include a wide variety of exogenous and endogenous factors such as natural disasters, technical failures, human errors, labor conflicts, sabotage, terrorism, acts of war [5]. A *threat* is a potential cause of an accident, such as line outage, bus-bar break, or overload, which may lead to a power system failure and possibly a loss of electric power for users. The conventional threats in power systems can be classified into two categories: *natural threats* and *accidental threats*. Natural threats include *meteorological problems* such as heat wave, tornado, lighting, and also *geological hazards* like earthquakes, tsunamis, landslides, volcanic eruption; accidental threats include such issues as *operational mistakes*, *maintenance failures*, and *equipment malfunctions*. However, as the increasing of recognition of the importance of power systems towards our model society, it gradually becomes a popular victim of malicious threats. *Malicious threats* refer to terrorism or crime including cyber-attacks, rioting, product tampering, explosions bombing, etc. Since the September 11, 2001, the resources and efforts, used to protect electric power systems against natural and accidental threats, have been shifted to respond the internationally concerned evolving malicious threats [6]. Moreover, as the evolution and transition of the power system itself, emerging threats are being witnessed and difficult to be categorized into those three groups, such as systematic threats.

* Corresponding author at: Dipartimento Energia, Politecnico di Torino, Torino 10129, Italy. Tel.: +39 0110907117; fax: +39 0110907199.
E-mail addresses: ettore.bompard@ec.europa.eu (E. Bompard), tao.huang@polito.it (T. Huang), YingjunWubyingjun.wu@polito.it (Y. Wu), mihai.cremenescu@transelectrica.ro (M. Cremenescu).

0142-0615/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijepes.2013.02.008

Although many measures for preventing conventional threats have been proposed to enhance the security of power systems [7–14], the power system is still facing quite severe threats caused by them. The Great East Japan Earthquake occurred on March 11, 2011 with a magnitude of 9.0, caused catastrophic damages to several nuclear power plants and thermal power plants. A total 21 GW power supply was interrupted by the Tokyo Electric Power Company (TEPCO); consequently, 4.4 million families in eastern Japan were put into the darkness. During the post-earthquake period, from March 14 to March 29, rolling blackouts had to be scheduled in most of Tokyo by the TEPCO due to the generation capacity deficiency [15]. In this regard, the power systems were insufficient to withstand impacts from these threats.

Rapid technological advances in recent years in power electronics, computer technology, telecommunications, and exotic materials have been promising to the development of power systems [16]. On the other hand, the changes in the power systems also provide growing opportunity for emergent threats against the security of the system. In addition, the threat of human attacks faced by power systems has become more serious [17,18]. For example, the integration of smart grid devices reliant on communications to control them is giving rise to the possibility of a cyber-attack [19]; and the increase in the share of electricity supply from intermittent renewable generation is changing the nature of the system and the associated security challenges [20,21]. Therefore, there is a demonstrable need to provide up-to-date classifications and assessments of conventional threats and emerging threats for the considerations of power system security issues.

In this paper, we focus on the classification and trend assessment of the sources of threats which jeopardize the security of power systems. The basic concepts and definitions of related nomenclatures in power system security issues are given firstly. Then the structure and operation of contemporary power systems, and the evolving scenarios are briefly introduced. According to our classification, a threat can be categorized into *natural*, *accidental*, *malicious*, or *other emerging* threats. Hence a general framework for classifying threats is proposed with description and possible impacts on power systems. Afterwards, over a hundred of major historic power outages world-wide are selected for evaluating the sources. Finally the trends of each threat category, conventional and emerging, are investigated for the concern of future power systems security.

Accordingly, the rests of this paper are organized as follows: Section 2 gives a survey and proposed perspectives of relevant taxonomies regarding the issue of power system security. In Section 3, the evolving scenarios for power system are summarized. Section 4 provides definitions and examples for various threats. A general framework of classification of the sources of threats is proposed in Section 5. Then selected major historic power outages were employed to analyze the trends of threats to power system using the proposed framework in Section 6. After that, Section 7 was dedicated to a general suggestion of preventive and counteractive measures for power systems against threats. Finally, some conclusions were drawn in Section 8.

2. Basic taxonomies

As the power systems is evolving in many directions, such as network interconnections between nations or regions, utilizations of new technologies and controls, and operation in highly stressed conditions, different academic/industrial organizations proposed various definitions for some terminologies based on the scenarios in their own interests. This section intends to give a brief literature overview and our views of the concepts and definitions of associated terminologies in power system security issues.

2.1. A definition survey from literature

A survey of definitions of relevant terminologies for power system security issues from four academic/industrial organizations, namely IEC (the International Electrotechnical Commission), IEEE (the Institute of Electrical and Electronics Engineers), ENTSO-E (the European Network of Transmission System Operators for Electricity), and NERC (the North American Electric Reliability Corporation), is conducted (Table 1).

2.2. Proposed taxonomies

The survey shows that there are differences among the definitions of a same terminology from various academic/industrial organizations. In order to unify the understanding we propose our perspectives on these terminologies as below.

Reliability refers to the ability to supply loads with high level of probability for a certain time interval. It can be described by two attributes: security and adequacy. *Security* means the ability to withstand imminent disturbances or contingencies, such as electric short circuits or unanticipated loss of system elements, without interruption of customer service; and *adequacy* means the ability to supply power to customers in various conditions, taking into account operational constraints. As a sub-item of security, *stability* refers to the ability to maintain or to regain a state of equilibrium after disturbances or contingencies. Here *disturbance* refers to an unplanned incident producing an abnormal system condition; and *contingency* refers to an unexpected failure or outage of a system component. In addition, *vulnerability* and *robustness* are frequently used to qualify the low reliability and the high reliability of the power systems respectively. Moreover, similar to the concept of reliability, *availability* refers to the ability to perform a required function under certain condition over a given time interval.

3. Evolving scenarios for power systems

The evolution of the contemporary power systems is towards a more intelligent, higher energy efficient, more economic and environment friendly direction. The inspiration and aspiration from society are the main driving forces to advance the development of the infrastructure at different levels and aspects. Most importance of them are: the reformation of the sources, characterized by high penetration of renewable energy; the appearance of a smarter and robust backbone transmission grids, also known as super grid; and the rapid emergence and development of autonomous and intelligent equipment in the distribution network, i.e. smart grid.

3.1. Renewable energy

Renewable energy is energy which comes from natural resources such as sunlight, wind, rain, tides, and geothermal heat, which are renewable (naturally replenished) [33]. The deployment of renewable energy would result in significant energy security and economic benefits.[34]. For example, renewable energy resources have a significant potential for energy efficiency, this would reduce energy import dependency to bring both energy security and economic benefits. For small-sized distributed generators (especially prosumers) with renewable resources, such as PV panels and wind turbines due to their vicinity and integration to the end-users, along with the smart grids implementations, it would greatly decrease the scales and consequences of blackouts. Furthermore, the self-healing features of smart grids would also accelerate the recovery and restoration of the system.

Table 1
Definitions from academic/industrial organizations.

	IEC	IEEE	ENTSO-E	NERC
Reliability	Probability that an electric power system can perform a required function under given conditions for a given time interval [22]	The probability of its satisfactory operation over the long run [23]	A general term encompassing all the measures of the ability of the system, generally given as numerical indices, to deliver electricity to all points of utilization within acceptable standards and in the amounts desired [24]	Able to meet the electricity needs of end-use customers even when unexpected equipment failures or other factors reduce the amount of available electricity [25]
Security	Ability of an electric power system to operate in such a way that credible events do not give rise to loss of load, stresses of system components beyond their ratings, bus voltages or system frequency outside tolerances, instability, voltage collapse, or cascading [26]	The degree of risk in its ability to survive imminent disturbances (contingencies) without interruption of customer service [23]	The ability to withstand sudden disturbances, such as electric short circuits or unanticipated losses of system components or load conditions together with operating constraints. Another aspect of security is system integrity, which is the ability to maintain interconnected operations [24]	The ability of the bulk power system to withstand sudden, unexpected disturbances such as short circuits, or unanticipated loss of system elements due to natural causes [25]
Adequacy	The ability of an electric power system to supply the aggregate electric power and energy required by the customers, under steady-state conditions, with system component ratings not exceeded, bus voltages and system frequency maintained within tolerances, taking into account planned and unplanned system component outages [27]	A system's capability to meet system demand within major component ratings and in the presence of scheduled and unscheduled outages of generation and transmission components or facilities [28]	The ability of a power system to supply the load in all the steady states in which the power system may exist considering standards conditions [24]	The ability of the electric system to supply the aggregate electrical demand and energy requirements of the end-use customers at all times, taking into account scheduled and reasonably expected unscheduled outages of system elements [29]
Stability	The ability of an electric power system to regain or to retain a steady-state condition, characterized by the synchronous operation of the generators and a steady acceptable quality of the electricity supply, after a disturbance due, for example, to variation of power or impedance [30]	The ability of an electric power system, for a given initial operating condition, to regain a state of operating equilibrium after being subjected to a physical disturbance, with most system variables bounded so that practically the entire system remains intact [23]	The ability of an electric system to maintain a state of equilibrium during normal and abnormal system conditions or disturbances [31]	The ability of an electric system to maintain a state of equilibrium during normal and abnormal conditions or disturbances [29]
Availability	The ability of an item to be in a state to perform a required function under given conditions at a given instant of time or over a given time interval, assuming that the required external resources are provided [32]	–	A measure of time during which a generating unit, transmission line, ancillary service or another facility is capable of providing service, whether or not it actually is in service [31]	–
Contingency	–	–	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical element [31]	The unexpected failure or outage of a system component, such as a generator, transmission line, circuit breaker, switch, or other electrical element [29]
Disturbance	–	–	An unplanned event that produces an abnormal system condition [31]	An unplanned event that produces an abnormal system condition [29]

Renewable energy is attracting more and more attention in recent years. In 2009, renewable electricity generation already accounted for 62% (17 GW) of all newly constructed power-generating capacity in Europe. In particular, wind energy installation, increasingly larger in size, accounted for 38% (10.2 GW) of all renewable energy growth [35]. The growth rate of renewable energy has been keeping at a double-digit for the recent 5 years. Moreover, should a more secure, diverse and sustainable energy mix is expected to be achieved, this trend needs to continue. EIA (Energy Information Administration) estimated that there would be a 3.1% annually increase in the share of electricity generated from renewable energy during the period from 2008 to 2035 all around the world [36]. It means 45% of global electricity will be generated from renewable energy by the year of 2035 [37].

3.2. Super grid

Although a universally accepted definition for super grid does not exist, the following consensus on features of a super grid is reached: flexibility in system balancing; high capacity for bulk power transmission; and geographically long distances. The vision of the future super grid can be generally described as: for transferring a large amount of electricity generated by renewable energy sources far away from centers of consumption, HVDC (High Voltage Direct Current) and storage technologies are commonly utilized to build multi-GW "highways" for improving transmission capacity and system security.

FOSG (the Friends of the Super Grid) proposed an idea to build a mainly DC based offshore super grid which was designed to transmit a large amount of electricity generated from renewable energy in remote areas such as UK's offshore to load centers in the North Sea [38]. The proposal consists of three phases to 2050. The undergoing first phase is to link the UK power network with other nation's networks such as Norway, and Germany. This will be done by connecting several AC collection grids to an AC cluster called "super-node" and linking the "super-node" to shore via several point-to-point HVDCs. A more ambitious super grid, called Medgrid, was launched in November 2008 to pursue a better

interconnection of North Africa and Europe and pump electricity generated from wind and solar power from the Sahara to European cities [39].

3.3. Smart grid

Similar to super grid, no commonly recognized definition of smart grid exists. Different versions were proposed by research organizations and institutes depending on their own perspectives. The IEEE proposed the concept of smart grid as integrating many advanced technologies into power systems: "Smart grid refers to the next-generation, managed electrical power system that leverages increased use of communications and information technology in the generation, delivery and consumption of electrical energy" [40]. The idea of smart grid from EPRI (the Electric Power Research Institute) is more or less the same as that from the IEEE: "An intelligent electric power delivery infrastructure (Intelligent Grid) that integrates advances in communications, computing, and electronics to meet society's electric service needs in the future" [41]. However, FERC (the Federal Energy Regulatory Commission) emphasizes smart grid on the consumers: "The smart grid concept envisions a power system architecture that permits two-way communication between the grid and essentially all devices that connect to it, ultimately all the way down to large consumer appliances" [42]. In contrast, the version of smart grid from DOE (U.S. Department of Energy) much focuses on its functionality: "A Smart Grid is self-healing, enables active participation of consumers, operate resiliently against attack and natural disasters, accommodate all generation and storage options, enable introduction of new products, services and markets, optimize asset utilization and operate efficiently, provide power quality for the digital economy" [43]. Unlike the US versions, the ETP (European Technology Platform) pays its attention to actors in the smart grid: "Electricity networks that can intelligently integrate the behavior and actions of all users connected to it – generators, consumers and those that do both – in order to efficiently deliver sustainable, economic and secure electricity supplies" [44].

In 2004, a project was launched to implement the integration of advanced metering management system into power systems for improving energy efficiency in Italy. High accuracy bidirectional meters and smart grid applications, such as network operation control and automatic low/medium voltage online status monitor, were included in the project [45]. The project SmartGridCity launched by Xcel Energy in 2008 in the US was another technology pilot that explored smart grid tools in a real-world setting. The goals of the project were to find out the energy management and conservation tools customers' preferred, the most effective technologies to delivery electricity, and the best ways to incorporate smart grid technologies into the business operations. For instance, approximately 23,000 smart meters in Boulder were installed for better electricity grid management in the project [46]. In addition, China's Tianjin Electric Power Company started Smart Grid Demonstration Project in Sino-Singapore Tianjin Eco-city in 2010. A smart power supply grid with a 220 kV and 110 kV transmission network, a 10–35 kV medium-voltage distribution network, and a 380 V/220 V low-voltage distribution network was completed by the year 2011 [47].

4. Threats to power systems

Through the analysis of relevant terminologies of power systems security issues in previous sessions, it can be found that the concepts and the origins of threats are not specially stressed. However, as a matter of fact, increasing blackouts caused by various threats have been witnessed in recent decades. Therefore, there is a need to define and classify the threats and their origins.

A threat refers to a potential cause of an unwanted incident which may result in jeopardizing a power system. Generally, threat can be classified into four categories: natural threat, accidental threat, malicious threat, and emerging threat.

- *Natural threat*: natural disasters not strictly controlled by human that if happen may impact the power system operation causing damages (geomagnetic storms, earthquakes, forest fires, tsunamis, hurricane, flood, lightening, hail, animal, etc.).
- *Accidental threat*: failure of network devices and the wrong human decisions that may threaten power system secure operation (operational fault, system equipment failure, accident due to the poor management, etc.).
- *Malicious threat*: intentional actions against power system facilities and operations which are undertaken by different agents (terrorist, criminal group, cyber attackers, copper theft, vandal, psychotic, malware writer, etc.) by various means (explosives, high power rifles, malware, etc.) with willingness to cause damage for political or economic benefits.
- *Emerging threat*: the threat emerged with the evolution of power system such as the integration of renewable energy and the interdependency between power system and other infrastructures.

Usually, natural threat and accidental threat are catalogued as conventional threat; and malicious threat and emerging threat are treated as unconventional threat (although some of the malicious threats are also conventional, such as sabotage and vandalism). Here we propose the concept of conventional threat and unconventional threat as follows:

- *Conventional threat*: potential incidents that have threatened power systems for a long time as the development of power systems.
- *Unconventional threat*: potential incidents that are becoming apparent, important, or prominent in very recent time due to the interior or exterior factors, such as terrorism, the evolution of power systems, the innovation of technology.

4.1. Natural threat

The cause of a natural threat is linked to power system's exposure to the geographically locational environment. An accident caused by natural threat is mainly because of *natural phenomena*, such as atmospheric discharges, lighting, winds, rather than a human factor. There were a series of large-scaled blackouts caused by natural threats all around the world. On September 28, 2003, a flash-over between a conductor cable and a tree was excited by storms. The flash-over, along with erroneous human decisions, finally caused a serious power outage that affected all of Italy. The outage lasted for 12 h and a total of 56 million people were affected [48]. On January 8, 2005, the power supplied to more than 400,000 local residences in southern part of Sweden was lost due to the hit of a powerful hurricane. The blackout resulted in an economic loss of hundreds of millions in Swedish Kronor [49]. Furthermore, in 2008, a combination of sustained low temperature, freezing rain and snowstorm hit southern China. The bad weather caused a large amount of transmission lines and towers physically damaged. As many as 13 provinces were affected and approximately 169 counties were put into the darkness in this blackout. The direct economic loss of this blackout was estimated to be more than 100 billion RMB [50]. Last year, the catastrophic nuclear leakage accident in Japan system named "Japan Nuclear Crisis", caused by earthquake and tsunami, caught the eyes of the whole world [15].

4.2. Accidental threat

The causes of an accidental threat can be either an *equipment failure*, such as a breaker rejecting movement, an insulator breakdown, an overload of a transformer, or an *operational fault*, such as a human error or mistake in system planning, operation, or maintenance. On September 8–9, 2011, a monitoring equipment failure caused problems at a power substation in southwest Arizona which finally led to a widespread power outage. It affected parts of Southern California and Arizona, as well as parts of northwestern Mexico [51]. The 2003 Northeast Blackout is an example for the cause of operational faults. A high-voltage power line was shut down due to a mis-operation by the TSO, followed by a cascade of failures throughout southeastern Canada and Northeast USA [3].

4.3. Malicious threat

Power system is becoming a popular target of malicious attack for various reasons, such as criminal, military or political purposes as the incapacity or destruction of it would have impacts on debilitating national economic security and national safety. Power systems can be sub-divided into three layers: physical layer, human layer, and cyber layer. Physical layer refers to tangible properties related with electric power, such as power plants, transmission lines, and transformers; human layer refers to the personnel who have access to the power systems; and cyber layer includes the information hardware, software, data, and the communication networks supporting the function of electric power system. A malicious threat is always implemented on/through/by the three layers, such as the destruction of transformers at the physical layer, damages caused by malicious insiders at the human decision layer, attacks through malwares, and hacking at the cyber layer. From 1999 to 2002, there were over 150 deliberate attacks on electric power system all around the world [52]. Tables 2 and 3 nonexclusively list malicious attacks to power systems in the USA and other parts of the world, respectively.

There was a report from Dept. Energy: averagely 39 attacks per year (totally 386) happened on U.S. energy assets from 1980 to 1989, most of which targeted at power systems [53]. Although no further official report of malicious threats to American power system can be found, according to our analysis in Section 6, we believe the attack rate is far more frequent nowadays than before.

4.4. Emerging threat

It is impossible to provide all emerging threats as some of them are still unobserved. Here, from the view of threat from exterior or interior power system, we propose two kinds of emerging threats.

4.4.1. Systemic threat

Renewable energy, such as wind power and solar power, is increasingly used to generate electricity. The integration would threaten the security of power system due to the intermittent characteristic of renewable sources. For example, it would be a challenging task for the system operator to maintain the balance between generation supply and real-time demand with large-scaled variable generation resources. Furthermore, the integration would affect the operational schedule for power systems. For instance, the intermittent energy resource is not completely dispatchable as conventional energy resources and the prediction of it is far from accuracy; therefore, the day-ahead operational schedule has to account for these factors for security reasons [54]. Additionally, high penetration of renewable energy into power markets brings incompatibilities between existing markets and new demand. For example, the EU power markets would be incompatible with the required rate of development to meet its 2020 aspirations. The incompatibilities include three aspects: low utilization rate of the network transmission capacity may increase the cost of renewable energy connection; not improved wind forecast techniques used during system dispatching optimization might worsen the system security; no transparent system constraints signals are revealed to transmission network investment decisions [55].

Another new development of modern power system is the **Smart Grids. With the requirements of supporting increasing situational awareness and allowing finer-grained command and control, an extensive computer and communication infrastructure needs be developed and deployed in the Smart Grids. This would raise numerous challenges involving quite complex interactions with the integration of cyber and physical systems [56], and also relating to cyber-security of systems due to the increasing potential of cyber-attacks and incidents against the critical infrastructure [57,58]. Specially, three types of malicious threats on the infrastructure, namely network availability, data integrity, and information privacy, are classified and evaluated in paper [59].

4.4.2. Impacts from other infrastructures

Infrastructures, such as electric power, water, oil, telecom, transportation, and natural gas, are becoming increasingly interconnected with each other. This interdependence means that an accident in one infrastructure may rapidly create global effect by cascading into other infrastructures. Therefore, the interdependence would pose new threats for the security of power system. For example, natural gas is becoming a primary fuel source of on-peak capacity in power systems [60]. The reliance on the natural gas supply would seriously affect the security of power system. When an interruption happened in gas pipeline system, it may lead to a loss of gas-fired electric generators [61].

Table 2
Malicious attacks happened in the USA.

Time	Site	Event	Attack type	Damage level
1981	Florida	Two substations were heavily damaged by simultaneous dynamite explosions in one of the most expensive incidents	Physical	Components damage and blackout
1986	Arizona	Three 500-kV lines from the Palo Verde Nuclear Generating Station were grounded simultaneously over a 30-mile stretch	Physical	Components damage
1987	California	Cutting of guy wires and subsequent toppling of a tower on the 1800-MW, 1000-kV DC intertie	Physical	Components damage
1989	Kentucky	A tower on a 765-kV line owned by the Kentucky Power Co. was bombed, temporarily disabling the line	Physical	Components damage
2005		Security consultants within the electric industry reported that hackers were targeting the US electric power grid and had gained access to US utilities' electronic control systems	Cyber	No actual damage
2010	Ohio	The thieves cut a hole in the fence and took copper grounding wires, shut off power	Physical	Components damage and blackout
2011	New Mexico	Copper thieves ripped off Socorro Electric Cooperative, stripping ground wire from poles in the Tierra Grande area	Physical	Components damage

Table 3
Malicious attacks happened in other countries.

Time	Site	Event	Attack type	Damage level
2002		Cigre conducted an international study of power substation security. Out of their 40 respondents 35 reported that they had at least one unauthorized intrusion annually	Physical	
2003	Long quan, China	Virus spread in the Control system of converter station	Cyber	No actual damage
2003	Corrs Corner, UK	A substation has been attacked a number of times during the last 2 months by vandals throwing stones at electricity equipment on the site. It had resulted in damage to equipment installed in the high voltage substation	Physical	Components damage
2004	Mosca, RUS	Bomb against electric lines tower	Physical	Components damage
2004	Irun, ES	Bomb against high voltage tower	Physical	Components damage
2004	Baghdad, IRQ	Explosion of three car bombs during the ceremony for the inauguration of a water plant (42 dead, 140 wounded)	Physical	Death of staff and components damage
2005	Qinghai, China	According to the statistics, in 2005, 137.11 km cable, 15 transformer, 60 solar panels and 3840 steel blocks of tower are stolen	Physical	
2006	Sos del Rey Catolico, ES	Bombs against a hotel and an electric substation	Physical	Components damage
2006	Jaca, ES	Bomb against a power plant	Physical	Components damage
2006	Nahrawan, IRQ	Malicious attacks against a power plant (9 dead, 2 wounded)	Physical	Death of staff and components damage
2006	Baiji, IRQ	Attacks against three engineers of a city power plant (3 dead)	Physical	Death of staff and components damage
2006	Taji, IRQ	Attacks against three engineers of a power plant (3 dead)	Physical	Death of staff and components damage
2006	Ba'qubah, IRQ	Bomb against some officers of an electric company (5 dead, 6 wounded)	Physical	Death of staff and components damage
2006	Baghdad, IRQ	Attacks against a minibus of officers of the power plant (3 dead, 6 wounded)	Physical	Death of staff and components damage
2008	Elizabeth Downs, Australia	Offenders broke into a high-voltage substation and stole valuable copper wiring. Blackouts spread from Elizabeth and Gawler, into the Adelaide Hills and as far south as Kilburn	Physical	Components damage and blackout
2009	South East London and North Kent, UK	The vandals deliberately caused a fire near a cable installation, which caused failure of a 132 kV cable and four circuit boards. As a result, power supplies were cut to around half of the homes for around 4 days, whilst other homes were given 3 h allocations of power followed by 6 h "off"	Physical	Components damage and blackout
2010	Bushehr, Iran	30,000 industrial computer systems of the nuclear reactor project of Iranian Bushehr Nuclear Power Plant had been infected by the Stuxnet virus. The first-known cyber attack targeted at power systems	Cyber	No actual damage
2010	Bolton, Greater Manchester, UK	An electrical surge caused by copper thieves led to a power cut for almost 400 properties in Bolton	Physical	Components damage and blackout
2010	Ronchin, France	Four copper thieves stole 1.86 miles of electric cables which made 118 trains delayed	Physical	Components damage and trains delayed

5. Threat catalogue

A blackout caused by any threat can be generalized by a chain: firstly, an event would be caused by a threat; then it results in variations of effects on power systems; finally, blackout happens due to a certain phenomenon. In this paper, *event* refers to the topological change of power systems, the alteration of components operational status; *effect* refers to the shift of power system state in terms of electrical qualities; and *phenomenon* refers to the essential reason resulting in the blackout.

5.1. Natural threats classification

A classification regarding to natural threats is given in Table 4. The threats are categorized according to their natural quality, and corresponding descriptions and possible impacts on power systems are also provided for each threat.

5.2. Accidental threats classification

A classification regarding to accidental threats is given in Table 5 with simple descriptions and possible impacts on power systems for each. We subdivide operational fault into three subcategories: design error, operation mistake, and maintenance accident. Likewise, equipment failure is subdivided into three subcategories: equipment defect, technical failure, and human/animal interference.

5.3. Malicious threats classification

According to the three layers of power system, malicious threats can be classified into physical threat, human threat, and Cyber threat. The classification is given in Table 6 with corresponding descriptions and possible impacts on power systems for each one.

5.4. Emerging threats classification

Two kinds of emerging threats, systemic threat and impacts from other infrastructures, listed in Table 7 represent the threat brought by internal and external factors.

6. Blackouts trend analysis

6.1. Selection of the representative blackouts

It is impossible to review all power blackouts happened in history due to the enormous quantity. In this section, the blackouts to be considered must conform to following criteria:

- The affected population must be larger than 1000 inhabitants.
- The duration must be longer than 1 h.
- The affected population times the duration must be larger than 1,000,000 inhabitant-hour.

By the criteria, 133 blackouts happened during the period from 1965 to 2011 have been selected as the representatives of major

Table 4
Classification of natural threats.

Threats categories		Descriptions	Possible Impacts
Geological disasters	Avalanche	A sudden flow of snow down a slope, occurring when either natural triggers or human activity causes a critical escalating transition from the slow equilibrium evolution of the snow pack	Damaging/malfunctioning power systems equipment/ installations (overhead lines, outdoor substations, power units, etc.)
	Earthquake	Earthquake is a sudden shake of the Earth's crust caused by the tectonic plates colliding	Damaging/malfunctioning power systems equipment/ installations (lines, outdoor substations, power units, etc.). Severely, the damages could extend to control centers of the entire power systems. Also, resulting in other threats like chemical contamination, pollution or earthquakes to hazard power systems
	Volcanic eruptions	An ejection of lava, tephra (volcanic bombs, lapilli, and ash), and various gases suddenly or dramatically from a volcanic vent or fissure	Damaging/malfunctioning power systems equipment/ installations (lines, substations, power plants, power units, control centers, etc.)
	Landslide	A geological phenomenon of ground movement, such as rock-falls, deep failure of slopes and shallow debris flows, which can occur in offshore, coastal and onshore environments	Damaging/malfunctioning power systems equipment/ installations (overhead lines, outdoor substations, power units, etc.)
Hydrological disasters	Flood	An overflow or high level of an expanse of water that submerges land	Damaging/malfunctioning power systems equipment/ installations (lines, substations, power plants, power units, control centers, etc.)
	Limnic eruption	A suddenly erupts of suffocating or inflammable gases saturated with carbon dioxide and other gases (i.e. methane) from deep lake water	Affecting human health, individual physiological and psychological conditions, even leading to death to cause people losing the capability to carry out operational activities (delivering operational signals from control centers, network, adjusting generation units in power plant, etc.) by suffocating employees. Also, resulting in other threats like tsunamis in case of very large lakes
	Tsunami	A series of water waves caused by the displacement of a large volume of a body of water, usually an ocean, though it can occur in large lakes	Damaging/malfunctioning power systems equipment/ installations (lines, substations, power plants, power units, control centers, etc.)
Meteorological disasters	Blizzard	A severe blizzard with strong wind, driving heavy snowfall and ice, intense cold, covering a wide area which moves more or less rapidly to neighbor regions	Damaging/malfunctioning power systems equipment/ installations (switching devices, overheard line, insulators, towers, etc.) Deteriorating the conditions of power systems normal and safe operations (power balance, power system security, etc.) caused by hydropower generation capacity decrease because of water freezing or by industrial and household electrical heating consumption increases. Worsening the maintenance intervention condition. Also, resulting in other threats like ice storm or cold wave may be possible
	Windstorm	A storm marked by high wind with little or no precipitation	Damaging/malfunctioning power systems equipment/ installations (switching devices, overheard line, insulators, towers, etc.) Deteriorating the conditions of power systems normal and safe operations (power balance, power system security, etc.) caused by hydropower generation capacity decrease because of water freezing or by industrial and household electrical heating consumption increases. Worsening the maintenance intervention condition
	Cyclonic storm	A violent hurricane of limited diameter created by winds rotating inwards to an area of low barometric pressure	Damaging/malfunctioning power systems equipment/ installations (overhead lines, outdoor substations, power plants, power units, communication sites, etc.)
	Drought	An unusually extended period of time when a region notes a deficiency in rain cause lacking of water in the rivers	Impacting power generation (especially on hydrogenation, but also on thermal or nuclear generation in cooling conditions). Deteriorating the conditions of power systems normal and safe operations (power balance, power system security, etc.) caused by irrigation and water pumping. Also, resulting in other threats like wild fires or famines
	Hailstorm	A drop of heavy hails	Damaging/malfunctioning power systems equipment/ installations (overhead lines, outdoor substations, power plants, communication sites, etc.)
	Heat wave	A heat wave is a prolonged period of excessively hot weather, which may be accompanied by high humidity	Worsening technical working condition of power system equipment/installation (cooling condition of power devices and IT or communication equipment, dilating overheard lines sag over tolerable limit, etc.). Deteriorating the conditions of power systems normal and safe operations (power balance, power system security, etc.) caused by generation capacity decrease because of bad cooling conditions of thermal/nuclear power units or by air conditioning and household cooling consumption increase
	Tornado	A violent, dangerous, rotating column of air that is in contact with both the surface of the earth and a cumulonimbus cloud or, in rare cases, the base of a cumulus cloud	Damaging/malfunctioning power systems equipment/ installations (overhead lines, outdoor substations, power plants, power units, communication sites, etc.)
	Lightning	An atmospheric electrostatic discharge (spark) accompanied by thunder, which typically occurs during thunderstorms, and sometimes during volcanic eruptions or dust storms	Damaging/malfunctioning power systems equipment/ installations (overhead lines, outdoor substations, power plants' external equipment, communication sites, etc.)
	Rainstorm/	A transient storm of lightning and thunder, usually with rain	Damaging/malfunctioning power systems equipment/

Table 4 (*continued*)

Threats categories		Descriptions	Possible Impacts
	thunderstorm	and gusty winds, sometimes with hail or snow, produced by cumulonimbus clouds	installations (overhead lines, outdoor substations, power plants, communication sites, etc.). Also, resulting in other threats like rainstorm or lightning
	Cold storm	A prolonged period of excessively cold weather	Worsening technical working condition of power system equipment/installations (locking switching devices driving, etc.). Deteriorating the conditions of power systems normal and safe operations (power balance, power system security, etc.) caused by hydropower generation capacity decrease because of water freezing or by industrial and household electrical heating consumption increase. Worsening the maintenance intervention condition
	Ice storm	A storm of freezing rain and widespread glaze formatted by snow or rain, forming a coat of ice on the surfaces it touches	Damaging/malfunctioning power systems equipment/ installations (blocking switching devices driving, mechanical overloading of overheard lines, breaking of insulators and towers, etc.). Also, resulting in other threats like cold wave
Fires	Wildfire	A uncontrolled fire in combustible vegetation that occurs in the countryside or a wilderness area	Damaging power systems equipment/installations (lines, substations, power plants, power units, communication sites, control centers, etc.)
Health disasters	Epidemic	A contagious disease that spreads rapidly in a community/ human population at a particular time	Affecting human health, individual physiological and psychological conditions, even leading to death, to cause people losing the capability to carry out operational activities (control centers, network, power plant and electricity production, communication and IT services, maintenance, etc.) by causing employees' illness and death
	Pandemic	An epidemic over a large area (prevalent throughout an entire country, continent, or the whole world)	Affecting human health, individual/social physiological and psychological conditions, even leading to death, to cause people losing the capability to carry out operational activities (control centers, network, power plant and electricity production, communication and IT services, maintenance, etc.) by causing employees' illness and death at extended geographical dimensions
	Famine	A widespread scarcity of food in a country or over a large geographical area, for a great number of people, causing illness and death, caused by wars, terrorist coordinated actions, epidemics, pandemics, geological or meteorological widespread disaster	Affecting human health, individual/social physiological and psychological conditions, even leading to death, to cause people losing the capability to carry out operational activities (control centers, network, power plant and electricity production, communication and IT services, maintenance, etc.) by causing employees' illness and death
Space disasters	Impact event	A collision of a large meteorite, asteroid, comet, or other celestial object with the Earth or another planet	Affecting human health, individual/social physiological and psychological conditions, even leading to death, to cause people losing the capability to carry out operational activities (control centers, network, power plant and electricity production, communication and IT services, maintenance, etc.) by causing employees' injuries and deaths. Damaging/malfunctioning power systems equipment/installations (blocking switching devices driving, mechanical overloading of overheard lines, breaking of insulators and towers, etc.)
	Solar flare/ magnetic storm	A sudden powerful eruption of particles and electromagnetic radiation (e.g. solar gases, cosmic rays, X-rays, gamma rays and magnetic storms, charged particles, etc.) from the Sun surface	Affecting/malfunctioning power devices/communication equipment operate on magnetic induction basis (autotransformers, measuring devices, etc.) by magnetic interference to cause transformer saturation, geomagnetic induction currents in HV transmission lines, current flowing through the earth along HV transmission lines, static compensator instability, subsequent voltage distortion and oscillation or power swing, fake actuating pulses on gears, protective relays and automations, communication failures including satellite links. Also, resulting in geomagnetic disturbances to cause a widespread tripping of key transmission lines and irreversible physical damage to large transformers
	Gamma ray burst	A flash of gamma rays associated with extremely energetic explosions that have been observed in distant cosmos	Affecting power system only theoretically, no evidence in industry proves it
Contaminations	Bio/chemical contamination	The presence of an unwanted constituent (contaminant, poisonous or polluting) in material, physical body, natural environment, at a workplace, etc.	Affecting human health, even leading to death, to cause employees losing the capability to carry out operational activities (control centers, network, power plant and electricity production, communication and IT services, maintenance, etc.) by contaminating or poisoning employees. Affecting/damaging power systems insulating devices (insulation pollution, metal corrosion, others material erosion and/or chemical reactions and/or physical depositions, etc.). Damaging power systems equipment/installations (lines, substations, power plants, power units, communication sites, control centers, etc.)
	Radioactive contamination	An accident of radiation exposure when radioactive materials are released into the environment	Affecting human health, even leading to death and inherent forced evacuation of all the people in affected areas, to cause people losing the capability to carry out operational activities

(*continued on next page*)

Table 4 (*continued*)

Threats categories	Descriptions	Possible Impacts
		(control centers, network, power plant and electricity production, communication and IT services, maintenance, etc.) by contaminating or poisoning people. Affecting/malfunctioning power systems equipment/installations for a long time (lines, substations, power plants, power units, communication sites, control centers, etc.)

Table 5
Classification of accidental threats.

Accidental threats		Descriptions	Possible Impacts
Operational fault	Design error	Errors in the stages of system planning, decision making, system evaluation, etc.	Failing to establish or maintain desired operational states or functionalities
	Operational mistake	Mistaking executions or commands by system operators and other operational staff, occurring in the stage of system real-time operation	
	Maintenance accident	An unintentional accident caused by violation on the rules, ordinances, standards, etc., during the maintenance works or installation	
Equipment failure	Equipment defect/aging	The defect or aging of power system equipment threatening their secure operation	Causing power systems losing functionality through unexpected, dangerous, erroneous or harmful consequences over the equipment and installations
	Technical failure	A breakdown or ceasing of equipment caused by internal factors of the equipment with direct malfunctioning effects on each sector in power systems	
	Human/animal interference	An event to an installation caused by animals/human, creating electrical arc ignition, short circuits, explosions, equipment destruction, etc., leading to equipment breakdown, failures, accidental outages, tripping, etc.	
	Interior fire/explosion	The fire or explosion excited by operating equipment/ installations, but natural factors	

Table 6
Classification of malicious threats.

Malicious threats		Descriptions	Possible impacts
Physical threat	Terrorist attack	A violent act intending to create terror for religious, political, economical or ideological goals. It includes destructing the physical infrastructure and hurting staff of power system	Causing power systems losing functionality
	War act	A military attack on a power system to disable its functionality	
	Sabotage	A criminal activity affecting the production, transmission, and distribution of electricity, such as cooper theft of metal items from transmission lines	
Human threat	Insider threat	A staff with access to a power system organization exploiting the vulnerabilities of the power system with the intention to cause harm	Destroying power systems desired state
Cyber threat	Malware	Software designed to disrupt operation, gather information, or gain unauthorized access with the intention to cause harm	Destroying power systems desired state Causing power system losing functionality
	Hacking	A hacking into cyber system to control power system with the intention to cause harm	

Table 7
Classification of emerging threats.

Malicious threats	Descriptions	Possible impacts
Systemic threat	The threat brought by the evolution of power systems	Increasing the uncertainty of power systems
Impacts from other infrastructures	Failures in other infrastructures spreading to power systems	

historic blackouts. A list of when, where, and what threats trigged the blackouts is given in Table 8.

A curve of the occurrences of blackouts along time is given in Fig. 1. As it can be observed, the frequency of historic blackout per very year remained fairly at the same level, nearly once a year, from 1965 to 1995. In the following decade, the frequency varied but stayed at a moderate high level. The years after 2005 witnessed a soar in the frequency to comparatively a high level, hovering around 17 blackouts per year. The ascending trend of the occurrences of blackouts in recent years suggests that today's power systems are becoming increasingly vulnerable to various threats.

Table 8
List of selected historic blackouts with their causes.

Dates	Locations	Threats	Dates	Locations	Threats
1965-11-09	Northeastern USA and Ontario, Canada	Maintenance accident	2007-04-26	Colombia, USA	Technical failure
1974-10-13	Nova Scotia, New Brunswick, etc., Canada	Blizzard	2007-06-27	New York City, USA	Lightning
1976-07-04	Utah, and southwestern Wyoming, USA	Technical failure	2007-06-27	long Island, USA	Rainstorm/thunderstorm
1977-07-13	New York City, USA	Lightning	2007-07-23	Barcelona, Spain	Technical failure
1978-12-19	France	Operation mistake	2007-07-25	Macedonia, Albania, Greece	Heat wave
1981-01-10	Utah, Idaho and Wyoming, USA	Human/animal interference	2007-08-20	Regina, Canada	Rainstorm/thunderstorm and lightning
1983-12-27	Sweden	Operation mistake	2007-09-26	Espírito Santo, Brazil	Hacking
1987-10-15	Southern England, UK	Blizzard	2007-12-02	Eastern Newfoundland, Labrador, Canada	Cold storm
1989-03-13	Quebec, Canada	Solar flares/solar winds/ magnetic storm	2007-12-08	Great Plains, USA	Ice storm
1990-12-07	English Midlands, UK	Blizzard	2008-01-04	Northern California, USA	Rainstorm/thunderstorm and cold storm
1991-07-07	Central North America, USA	Windstorm	2008-01-25	China	Blizzard and infrastructure interdependency
1995-10-04	Eastern and southern North America, USA	Cyclonic storm	2008-02-11	Southern Calgary, Canada	Ice storm
1996-08-10	Nine states of the United States; Parts of Mexico	Heat wave	2008-02-20	Jakarta, Indonesia	Infrastructure interdependency
1996-11-19	Washington and Idaho, USA	Ice storm	2008-02-26	Florida, USA	Interior fire/explosion
1998-01-xx	Northeastern North America, USA	Ice storm	2008-04-02	Melbourne and Victoria, Australia	Windstorm
1998-02-20	Auckland, New Zealand	Equipment defect/aging	2008-04-08	Szczecin, Poland	Blizzard
1998-05-31	Central North America, USA	Windstorm	2008-04-29	Venezuela	Technical failure
1998-09-25	Victoria, Australia	Infrastructure interdependency	2008-05-20	Island of Zanzibar, Tanzania	Equipment defect/aging
1998-12-08	San Francisco, USA	Maintenance accident	2008-06-24	Maidstone, UK	Technical failure
1999-03-11	Brazil	Lightning	2008-08-04	Chicago, Illinois and Northwest Indiana, USA	windstorm
1999-07-29	Taiwan, China	Landslide	2008-09-01	Venezuela	Technical failure
1999-10-29	Orissa, India	Cyclonic storm	2008-09-13	Texas, New York, USA	Cyclonic storm
1999-11-22	Tokyo and south of Saitama Prefecture, Japan	Human/animal interference	2008-11-11	Southern Louisiana, Massachusetts, etc., USA	Blizzard and ice storm
2000-05-09	Entire southern half of Portugal	Human/animal interference	2008-12-26	The entire island of Oahu, Hawaii, USA	Lightning
2001-05-20	Isfahan, Shiraz, Tabriz, etc., Iran	Heat wave	2009-01-23	France	Windstorm
2003-07-22	Memphis, Tennessee metropolitan area, USA	Windstorm	2009-01-27	Kentucky and Southern Indiana, USA	Ice storm
2003-08-14	Northeastern USA; Central Canada	Operation mistake	2009-01-27	Victoria, Australia	Heat wave
2003-08-28	Central and south London, UK	Equipment defect/aging	2009-03-06	Kent, UK	Technical failure
2003-09-19	Nine US states, USA; Parts of Ontario, Canada	Cyclonic storm	2009-03-28	Georgia, USA	Tornado
2003-09-27	Italy	Windstorm	2009-03-30	Sydney, Australia	Technical failure
2004-06-29	Northern, eastern and western parts of Singapore	Infrastructure interdependency	2009-03-30	Glasgow and West of Scotland, UK	Technical failure
2004-07-12	Lavrio and Megalopoli, Greece	Technical failure	2009-07-02	Australia	Technical failure
2004-09-04	Florida, USA	Cyclonic storm	2009-07-20	South East London and North Kent, UK	Sabotage
2005-01-13	Malaysia's northern peninsular	Technical failure	2009-10-08	North and west Melbourne, Australia	Operation mistake
2005-01-xx	North of Rio De Janeiro, Brazil	Hacking	2009-10-30	Northland and northern of Auckland, New Zealand,	Human/animal interference
2005-01-08	Sweden	Windstorm	2009-11-10	Brazil	Rainstorm/thunderstorm
2005-05-25	Moscow, Russia	Interior fire/explosion	2009-11-23	Northeastern Tennessee, USA	Blizzard
2005-06-16	Puerto Rico	Technical failure	2010-01-30	Darwin, Katherine and Palmerston, Australia	Lightning
2005-08-18	Java Island, Indonesia	Technical failure	2010-02-05	Northeastern USA	Blizzard
2005-08-22	Southern and central Iraq	Sabotage	2010-03-06	Melbourne, Australia	Windstorm/hailstorm
2005-08-26	South Florida, USA	Cyclonic storm	2010-03-14	Chile	Technical failure
2005-08-29	Louisiana, Mississippi and Alabama, USA	Cyclonic storm	2010-03-14	Southwestern Connecticut, Westchester, Long Island, and New Jersey, USA	Windstorm and rainstorm/ thunderstorm
2005-09-12	Los Angeles, USA	Operation mistake	2010-03-30	Northern Ireland	Cold storm
2005-10-24	South and Southwest Florida, USA	Cyclonic storm	2010-05-31	Sheffield, UK	Technical failure
2005-12-15	Atlantic Coast, USA	Ice storm	2010-06-27	Portsmouth, UK	Interior fire/explosion
2005-12-22	Niigata prefecture, Japan	Blizzard	2010-07-15	Southeastern Michigan, USA	Windstorm and rainstorm/ thunderstorm
2006-06-12	Central and eastern Auckland, New Zealand	Technical failure	2010-07-25	Washington, DC, USA	Windstorm and rainstorm/ thunderstorm

(*continued on next page*)

Table 8 (*continued*)

Dates	Locations	Threats	Dates	Locations	Threats
2006-07-17	Ontario and Quebec, Canada	Rainstorm/thunderstorm	2011-01-xx	Queensland, Australia	Flood
2006-07-18	Philadelphia, USA	Windstorm	2011-02-02	Texas, USA	Cold storm
2006-07-18	Queens, New York, and Westchester County, USA	Interior fire/explosion	2011-02-03	North Queensland, Australia	Cyclonic storm
2006-07-19	St. Louis, Missouri, USA	Windstorm and rainstorm/ thunderstorm	2011-02-04	Northeastern Brazil	Technical failure
2006-07-22	Parts of greater London, UK	Heat wave	2011-02-22	Christchurch, New Zealand	Earthquake
2006-08-01	Québec, Canada	Rainstorm/thunderstorm	2011-03-11	Japan	Earthquake and tsunami
2006-08-02	Southern and eastern Ontario, Canada	Rainstorm/thunderstorm and windstorm	2011-04-15	Southeast US	Windstorm and rainstorm/ thunderstorm
2006-08-14	Tokyo Metropolitan Area, Japan	Human/animal interference	2011-04-25	Southeast US	Windstorm and rainstorm/ thunderstorm
2006-10-12	Buffalo, New York, USA	Blizzard	2011-04-xx	Elizabethtown, Kentucky, USA	Tornado
2006-10-15	Hawaii, USA	Earthquake	2011-06-30	Chennai city, India	Technical failure
2006-10-24	Lima, Peru	Human/animal interference	2011-07-11	Cyprus	Interior fire/explosion
2006-11-04	Germany, France, Italy, Belgium, Spain and Portugal	Design error	2011-07-11	Chicago, USA	Windstorm and rainstorm/ thunderstorm
2006-11-15	British Columbia, Canada	Windstorm	2011-07-23	Northern Saskatchewan, Canada	Technical failure
2006-11-30	St. Louis, USA	Cold storm	2011-08-27	US Eastern seaboard	Cyclonic storm
2006-12-01	Parts of Ontario, Canada	Cold storm	2011-09-08	California, Arizona, and Mexico, USA	Technical failure
2006-12-01	Long Island, New York, USA	Interior fire/explosion	2011-09-15	South Korea	Heat wave
2006-12-15	Seattle, USA	Windstorm	2011-09-24	The north and central Chile	Technical failure
2007-01-12	Missouri, Michigan, and Oklahoma, USA	Ice storm	2011-10-30	The East Coast of the USA	Blizzard
2007-01-16	Victoria, Australia	Interior fire/explosion	2012-03-13	Boston Massachusetts, USA	Wildfire
2007-04-19	Costa Rica	Drought			

6.2. Statistical analysis of the threats

The statistical results of the origins of the selected blackouts are reported in Table 9.

It is manifest from Table 9 that windstorm, rainstorm/thunderstorm, blizzard, cyclonic storm, ice storm, cold storm, heat storm, and lighting were the most frequent causes for blackouts. The rests caused fewer blackouts (e.g. flood, wild fire, etc.), and some of which have never been an origin of a blackout (e.g. famine, etc.). Technical failure contributed to half of the blackouts caused by accidental threat. For malicious threat, only hacking and sabotage among other means of intentional attacks triggered blackouts in history. Similarly, only impacts from other infrastructures resulted in blackouts among emerging threats. It is obvious that only a few threats dominated in the causes of blackouts. Fig. 2 provides the 19 dominant origins which caused more than 94.6% of the selected blackouts.

The lines in Fig. 3 show the individual trends of the four catalogues triggering blackouts over the period from 1965 to 2011. The upward trends of blackouts caused by natural threats and accidental threats are more noticeable during the last two decades. For malicious threats and emerging threats, there were no blackouts caused by them before 1998. However, after 1998, malicious threats and other emerging threats started to emerge as the reasons for blackouts.

The pie chart in Fig. 4 demonstrates the percentages of the causes for blackouts. Natural threats and accidental threats accounted for 94% of blackouts in the collection, while only 6% of blackouts were resulted from emerging threats. According to this, natural threats and accidental threats are still the main origins for blackouts.

Although traditional threats are still the main causes for blackouts, it should not be taken as the reason to ignore emerging threats. Fig. 5 gives a comparison between the number of blackouts

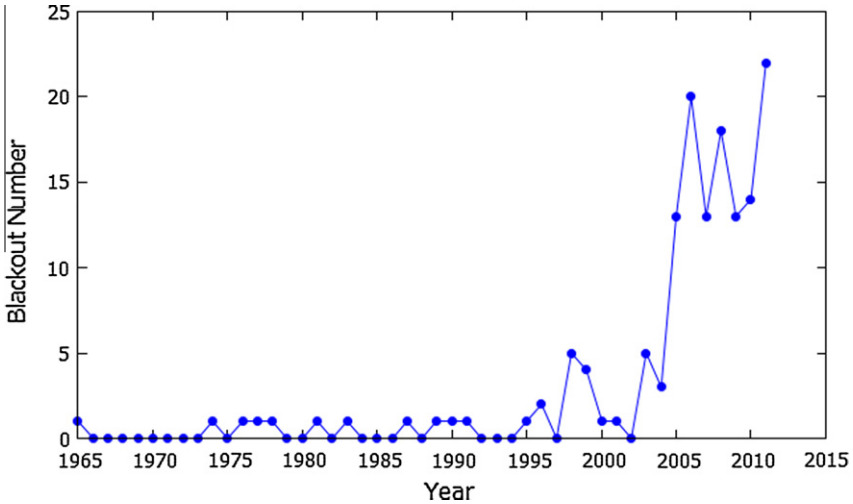

Fig. 1. The trend of blackouts in power systems.

Table 9
Statistics of the causes of the selected blackouts.

Category	Threats	Frequency	Category	Threats	Frequency
Natural	Windstorm	20	Natural	Pandemic	0
	Rainstorm/thunderstorm	14		Radioactive contamination	0
	Blizzard	11		Volcanic eruption	0
	Cyclonic storm	10		Avalanche	0
	Ice storm	8		Total	93
	Cold storm	6	Accidental	Technical failure	22
	Heat wave	6		Interior fire/explosion	7
	Lightning	6		Human/animal interference	6
	Earthquake	3		Operation mistake	5
	Tornado	2		Equipment defect/aging	3
	Drought	1		Maintenance accident	2
	Flood	1		Design error	1
	Hailstorm	1		Total	46
	Landslide	1		Hacking	2
	Solar flare/magnetic storm	1		Sabotage	2
	Tsunami	1		Malware	0
	Wildfire	1		Terrorist attack	0
	Bio/chemical contamination	0		War act	0
	Epidemic	0		Insider threat	0
	Famine	0		Total	4
	Gamma ray burst	0	Emerging	Impacts from other infrastructures	4
	Impact event	0		Systemic threat	0
	Limnic eruption	0		Total	4

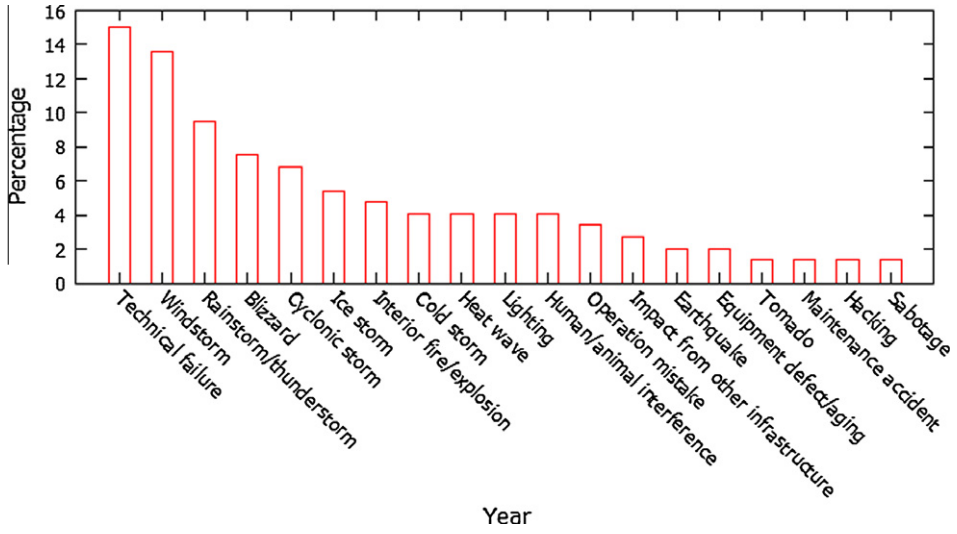

Fig. 2. The percentages of the selected blackouts caused by the 19 dominant origins.

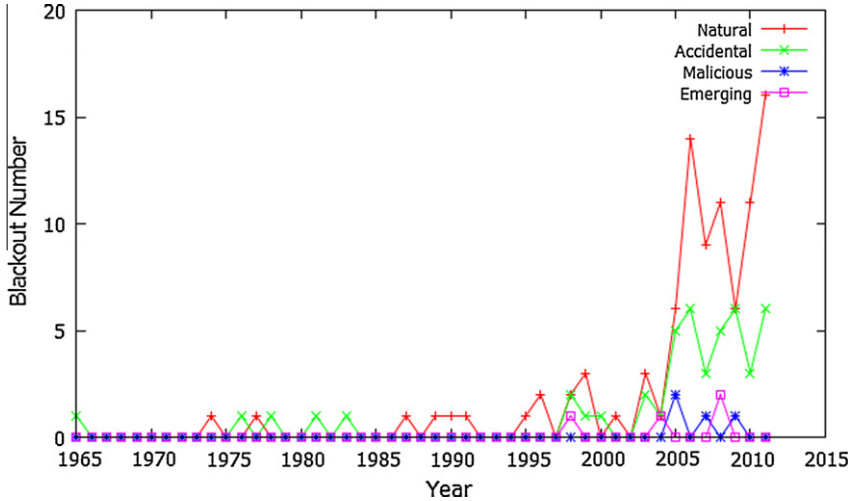

Fig. 3. Trends of four threat categories.

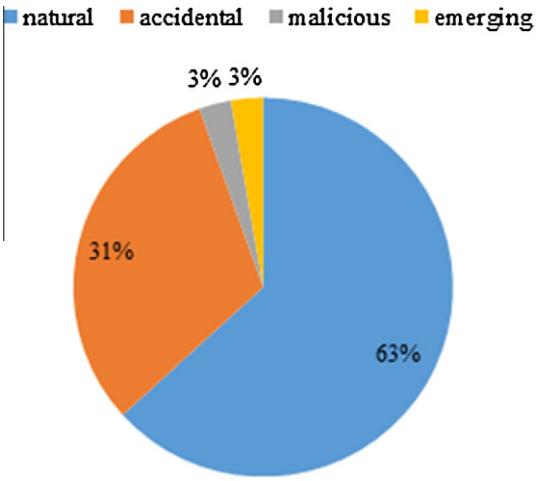

Fig. 4. Percentages of the causes for blackouts.

caused by conventional threats and emerging threats. As it can be seen from the graph, the last decade saw the take-off of the emerging threats as the contributors to blackouts.

7. Suggestions for power systems against threats

Due to the large geographical expansion of the power system and its high exposure to the environment, as well as the propagation of a local failure in the entire system at a light speed, the secure operation of the power system against threats have always been challenging to the operators and relative authorities. Facing with the complex problem, individual TSO has its own version of prevention and protection schemes. Yet, there are some general security policies that can be summarized in terms of defense strategies, including the security policies at various levels from utilities, TSOs, polices, law enforcement, governmental authorities, with special focus on malicious and intentional threats.

The general policies should cover various aspects of preventive and counteractive measures to establish and maintain the security level of power system operations, including:

- *Responsibility*: Staff for general, physical, cyber security should be clearly aware of the separately and appropriately predefined duties of their own.
- *Rules:* Guidance for security practice, including inspections and reliability tests, etc.
- *Training*: Programs to enhance the recognition for general and security staff of their responsibility and corresponding rules.
- *Self-assessments*: Evaluation of the state of the security program and each individual staff.
- *Emergency plans*: Quick response processes and plans for corrective control after the materialization of a threat, aiming at maximizing maintaining the functionality of the system as well as possibly limiting the damage.

More specifically, the following aspects are suggested in the industrial practices:

Reduction of system vulnerability: in the power systems planning and enforcing phase, making security as a design parameter could guide the evolution of future systems towards inherently less vulnerable technologies and configurations against different threats. Practically, the inherently less vulnerable technologies and design include using underground transmission lines/cables, standardized equipment, self-healing and intelligent equipment, etc. Besides, the reformation of the power system schemes should also towards a less vulnerable bulk power system as new facilities are planned and constructed (e.g. smart grids).

Preventing damages: the equipment itself and its location should be reinforced to resist damages, etc. For instance, key substations-protect critical equipment within walls or below grade should be hardened or even guarded; key pieces of equipment such as transformers need to be separated. Remote monitoring or surveillance on the key facilities coupled with rapid-response forces should be equipped. In the planning of the prevention, coordination with law enforcement and intelligence agencies should be improved to provide threat information and coordinated responses.

Limiting consequences: the contemporary operational practices after contingencies by TSOs and DSOs can be mainly considered as implementations regarding this catalogue. The emergency procedures for handling instability after major disasters should be improved along with the transition of power systems from traditional schemes towards new regimes. To limit the consequences, operators should modify the physical infrastructure, such as improving control centers and protective devices as the greater redundancy of key equipment, the more increased reserve and security margins.

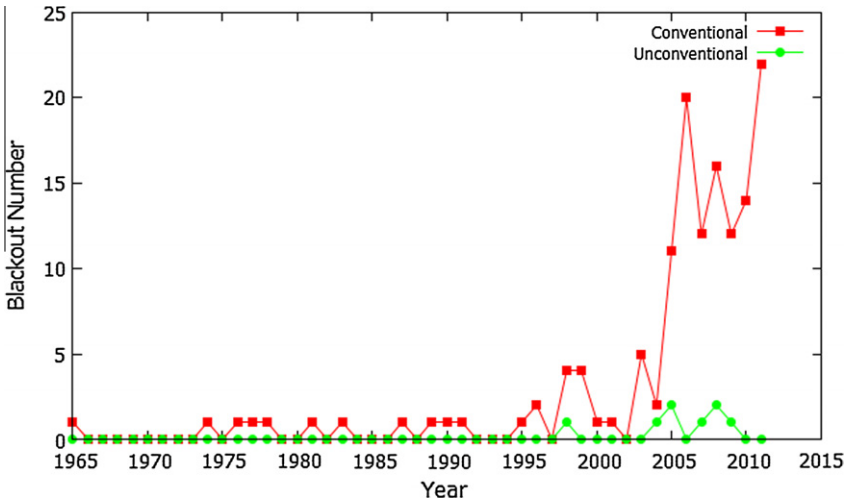

Fig. 5. Comparison between conventional and unconventional threats.

Speeding recovery: contingency planning for restoration of service is strongly advised. Legal/institutional framework for sharing reserve equipment should be clarified. The availability of adequate transportation for a stockpile of very heavy equipment for fast replacement should be assured. Domestic manufacturing capability should be monitored to make certain that adequate repair and manufacture of key equipment in times of emergency.

8. Conclusions

An overview of some taxonomies relating to the security of power systems is presented to provide a better understanding of the security issues of power systems. A survey of the definitions of these terminologies from some prestigious academic/industry organizations, such as IEC, IEEE, ENTSO-E, and NERC, is completed. Then, in order to unify the understanding, we propose our perspectives on these terminologies.

Conventional threats have been recognized for a long time in the secure operation of power systems. For example, a natural threat, such as atmospheric discharges, lighting, or winds, could cause the damage of a physical component resulting in the deterioration of the operative condition; an accidental threat, such as a breaker failure, an insulator breakdown, or a human error in system planning, could cause large-scale blackout; and a malicious threat, such a war, or an organized crime attacking the tangible properties of the power system, could much more sever damages and system-wise blackout. However, with the evolution of power systems and other changes, new threats are emerging. The integration of renewable energy into the power system would bring significant energy security and economic benefits, accompanied by great challenges to maintain the instantaneous balance between generation supply and real-time demand due to the intermittent characteristic of some renewable sources and difficulty to plan the operational schedule as the lack of techniques for predicting them in advance accurately. With a colossal number of small-sized ad hoc generation unites with intelligence, the traditional unidirectional energy transmission path from the generation to end users would change to a bidirectional scheme that end users would feed energy flows back to the transmissions; therefore, the contemporary ideology of control of the power system would be rendered obsolete. Moreover, the development of the Smart Grids, such as the deployment of a more advanced and sophisticated computer and communication infrastructure, is raising fundamental and far-reaching impacts on the power system, especially its security. It enables all the features of smart grids, but as well exposes the power system to more potential of cyber-attacks.

There was not a classification of threats reflecting these changes. Therefore, a detailed classification is proposed to meet the practical need. In the classification, natural threats, accidental threats, malicious threats, and emerging threats are divided into sub-threats according to their natural qualities, presentation mode, etc. In addition, a definition and a description of possible impacts on the security of power systems of each sub-threat are provided. We generalize the impacts of sub-threats in various ways, such as destroying physical infrastructure of power systems, affecting human physical health, deteriorating operational condition of power systems.

In the past decades, there was an increase in the number of blackouts all around the world. It means power systems are more and more vulnerable to various threats. Among these threats, windstorm, rainstorm/thunderstorm, blizzard, cyclonic storm, ice storm, cold storm, heat storm, and lighting belonging to natural threat, technical failure belonging to accidental threat, and hacking and sabotage belonging to malicious threat are the most threatening ones. Particularly, malicious threat such as hacking and emerging threat like impacts from other infrastructures started to cause blackouts in recent years. Although, conventional threat still dominates the causes of blackouts, enough attention should be paid to unconventional threat in the future.

Acknowledgements

This paper has been produced with the financial assistance of the SESAME project (a FP7-security project co-funded by the European Commission, aiming at providing a contribution to the development of tools and a regulation framework for the security of the European power grid against natural, accidental and malicious attacks. https://www.sesame-project.eu/). The views expressed herein are those of the SESAME consortium and can therefore in no way be taken to reflect the official position of the European Commission.

References

[1] Maas GA et al. System disturbance on 4 November 2006. Final, report; 2007.
[2] Rinaldi Steven M, Peerenboom James P, Kelly Terrence K. Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst Mag 2011;21:11–25.
[3] US–Canada Power System Outage Task Force. Final report on the August 14, 2003 blackout in the United States and Canada: causes and recommendations; 2004 April.
[4] Rosas-Casals Martí, Solé Ricard. Analysis of major failures in Europe's power grid. Int J Electr Power Energy Syst 2011;33:805–8.
[5] Halilcevic Suad S, Gubina Ferdinand, Gubina Andrej F. Prediction of power system security levels. IEEE Trans Power Syst 2009;24:368–77.
[6] The 9/11 Commission. Final report of the national commission on terrorist attacks upon the United States; 2004 July.
[7] McEachron KB. Lightning – a hazard to electric systems". Power Apparatus Syst 1952;71:977–82.
[8] Barnes HC. Tornadoes and transmission. IEEE Trans Power Apparatus Syst 1966;PAS-85:582–5.
[9] Albertson VD, Thorson JM, Clayton RE, Tripathy SC. Solar-induced-currents in power systems: cause and effects. IEEE Trans Power Apparatus Syst 1973;PAS-92:471–7.
[10] Eriksson AJ, Stringfellow MF, Meal DV. Lighting-induced overvoltages on overhead distribution lines. IEEE Trans Power Apparatus Syst 1982;101:960–8.
[11] Albertson VD, Thorson JM, Miske SA. The effects of geomagnetic storms on electrical power systems. IEEE Trans Power Apparatus Syst 1974;93:1031–44.
[12] Balijepalli N, Venkata SS, Richter CW, Christie RD, Longo VJ. Distribution system reliability assessment due to lightning storms. IEEE Trans Power Delivery 2005;20:2153–9.
[13] Huneault M, Langheit C, Caron J. Combined models for glaze ice accretion and de-icing of current-carrying electrical conductors. IEEE Trans Power Delivery 2005;20:1611–6.
[14] Kalyani S, Swarup KS. Pattern analysis and classification for security evaluation in power networks. Int J Electr Power Energy Syst 2013;44:547–60.
[15] Norio Okada, Ye Tao, Kajitani Yoshio, Shi Peijun, Tatano Hirokazu. The 2011 eastern Japan great earthquake disaster: overview and comments. Int J Disaster Risk Sci 2011;2:34–42.
[16] Horowitz S, Phadke A, Renz B. The future of power transmission. IEEE Power Energy Mag 2010;8:34–40.
[17] Salmeron Javier, Wood Kevin, Baldick Ross. Analysis of electric grid security under terrorist threat. IEEE Trans Power Syst 2004:905–12.
[18] Romero Natalia, Xu Ningxiong, Nozick Linda K, Dobson Ian, Jones Dean. Investment planning for electric power systems under terrorist threat. IEEE Trans Power Syst 2012;27:108–16.
[19] Kang DJ, Lee JJ, Kim BH, Hur D. Proposal strategies of key management for data encryption in SCADA network of electric power systems. Int J Electr Power Energy Syst 2011;33:1521–6.
[20] Degeilh Yannick, Singh Chanan. A quantitative approach to wind farm diversification and reliability. Int J Electr Power Energy Syst 2011;33:303–14.
[21] Xydis G. Comparison study between a renewable energy supply system and a supergrid for achieving 100% from renewable energy sources in Islands. Int J Electr Power Energy Syst 2013;46:198–210.
[22] The International Electrotechnical Commission. IEV number 617-01-01. International Electrotechnical Vocabulary; 2009 March.
[23] IEEE/CIGRE Joint Task Force on Stability Terms and Definitions. Definition and classification of power system stability. IEEE Trans Power Syst 2004;19:1387–401.
[24] The European Network of Transmission System Operators for Electricity [Internet]. Glossary of terms, statistical glossary. <https://www.entsoe.eu/resources/data-portal/glossary/> [cited 09.07.12].
[25] The North American Electric Reliability Corporation [Internet]. Company overview: FAQ. <http://www.nerc.com/page.php?cid=1%7C7%7C114> [cited 09.07.12].

[26] The International Electrotechnical Commission. IEV number 191-21-03. International Electrotechnical Vocabulary; 2009 March.
[27] The International Electrotechnical Commission. IEV number 191-21-01. International Electrotechnical Vocabulary; 2009 March.
[28] IEEE Working Group. Reliability indices for use in bulk power system supply adequacy evaluation. IEEE Trans Power Apparatus Syst 1978;PAS-97:1097–103.
[29] The North American Electric Reliability Corporation [Internet]. Glossary of terms used in nerc reliability standards. <http://www.nerc.com/files/Glossary_of_Terms.pdf.> [updated 25.05.2012, cited 09.07.12].
[30] The International Electrotechnical Commission. IEV number 617-01-03. International Electrotechnical Vocabulary; 2009 March.
[31] The Union for the Coordination of the Transmission of Electricity, glossary of terms, version 2.2; 2004 June.
[32] The International Electrotechnical Commission. IEV number 191-02-05. International Electrotechnical Vocabulary; 2009 March.
[33] The Renewable Energy Policy Network for the 21st Century [Internet]. Renewables 2011: global status report, 2011. <http://www.ren21.net/Portals/97/documents/GSR/GSR2011_Master18.pdf> [updated 2011 July, cited 09.07.12].
[34] International Energy Agency. Energy technology perspectives 2012. <http://www.iea.org/Textbase/npsum/ETP2012SUM.pdf> [cited 09.07.12].
[35] European Commission, Joint Research Centre, Institute for Energy. Renewable energy snapshots 2010; 2010 July.
[36] The U.S. Energy Information Administration. International energy, outlook 2011; 2011 September.
[37] International Energy Agency. World energy, outlook 2011; 2011 November.
[38] Aguado A. Towards a European supergrid. PSCC; 2011 August.
[39] Cole Stijn, Karoui Karim, et al. A European supergrid: present state and future challenges. 17th Power systems computation conference; 2011 August 22–26, Stockholm, Sweden.
[40] IEEE Smart Grid [Internet]. IEEE launches smart grid Web portal, content-rich gateway providing intelligence, education and news on global smart grid. <http://smartgrid.ieee.org/resources/ieee-press-releases/198-ieee-launches-smart-grid-web-portal-content-rich-gateway-providing-intelligence-education-and-news-on-global-smart-grid> [updated 19.01.10, cited 09.07.12].
[41] Bruno Sergio, Lamonaca Silvia, La Scala Massimo, Rotondo Giuseppe, Stecchi Ugo. Load control through smart-metering on distribution networks. IEEE Bucharest PowerTech conference; 2009 June 28–July 2, Bucharest, Romania.
[42] The Federal Energy Regulatory Commission. Proposed policy statement and action plan, smart grid policy. FERC Docket no. PL09-4-000; 2009 March.
[43] US Department of Energy [Internet]. Office of electricity delivery and energy reliability: "Smart Grid". <http://energy.gov/oe/technology-development/smart-grid> [cited 29.11.12].
[44] The European Technology Platform [Internet]. What is smart grids?. <http://www.smartgrids.eu/node/56#12> [cited 09.07.12].
[45] Smart Grid Information Clearinghouse [Internet]. Acea Distribuzione smart metering in Rome. <http://www.sgiclearinghouse.org/Europe?q=node/2583&lb=1> [cited 09.07.12].
[46] Xcel Energy [Internet]. SmartGridCity. <http://www.xcelenergy.com/smartgridcity> [cited 09.07.12].
[47] Sino-Singapore Tianjin Eco-city [Internet]. Introduction of the plan of Sino-Singapore Tianjin Eco-city. <http://www.eco-city.gov.cn/eco/html/zjstc/ztgh.html> [cited 09.07.12].
[48] Swiss Federal Office of Energy. Report on the blackout in Italy on 28 September 2003; 2003 November.
[49] Landstedt Jyrki, Holmström Petter. Electric power systems blackouts and the rescue services: the case of Finland. CIVPRO working paper 2007, vol. 1; 2007.
[50] South China Bureau of State Electricity Regulatory Commission. Power system operation condition report during 2008 snow disaster. Guangzhou, China, Tech. Rep.; 2008 February.
[51] Watson Julie, editors. Power failure leaves 5 million in the dark [Internet]. San Diego: The San Francisco Chronicle; 2011. <http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/09/08/MND01L2A1P.DTL> [cited 09.07.12].
[52] Zimmerman R, Restrepo CE, Simonoff JS, Lave L. Risk and economic costs of a terrorist attack on the electric system [Internet]. Presentation for the CREATE economics of terrorism symp; 2005. <http://create.usc.edu/assets/pdf/51818.pdf> [cited 09.07.12].
[53] US Congress. Office of technology assessment, physical vulnerability of electric system to natural disasters and sabotage, OTA-E-453 (Washington, DC: U.S. Government Printing Office; June 1990.
[54] International Energy Agency. Harnessing variable renewables: a guide to the balancing, challenge; 2011.
[55] House of Commons Energy and Climate Change Committee. A European supergrid. Vol. II, Seventh Report of Session 2010–2012; 2012.
[56] Khurana H, Hadley M, Ning Lu, Frincke DA. Smart-grid security issues. IEEE Secur Priv 2010;8:81–5.
[57] Metke Anthony R, Ekl Randy L. Security technology for smart grid networks. IEEE Trans Smart Grid 2010;1:99–107.
[58] Ericsson GN. Cyber security and power system communication—essential parts of a smart grid infrastructure. IEEE Trans Power Delivery 2010;25:1501–7.
[59] Lu Zhuo, Lu Xiang, Wang Wenye, Wang C. Review and evaluation of security threats on the communication networks in the smart grid. In: The 2010 military communications conference. p. 1830–5.
[60] The North American Electric Reliability Corporation [Internet]. 2011 long term reliability assessment; 2011 November. <http://www.nerc.com/files/2011LTRA_Final.pdf>.
[61] Shahidehpour M, Fu Y, Wiedman T, editors, Impact of natural gas infrastructure on electric power systems. Proceedings of the IEEE 2005 May.