Analysis of Chain of Events in Major Historic Power Outages

Tao Huang[1], Simona Louise Voronca[2], Anca Alexandra Purcarea[3], Abouzar Estebsari[1], Ettore Bompard[4]

[1]*Department of Energy, Polytechnic of Torino, Italy*
[2]*CN Transelectrica SA, Romania*
[3]*University Polytechnic of Bucharest, Faculty of Entrepreneurship, Business Engineering and Management, Romania*
[4]*European Commission, Joint Research Centre–Institute for Energy and Transport, Netherlands*
tao.huang@polito.it

Abstract— **Contemporary power systems are facing increasing intricate conditions that have never been considered when initially designing the infrastructure, such as malicious threats, accommodating smart grids, etc. As a consequence, blackouts albeit seldom but stubbornly keep appearing from time to time the world around, and demonstrate their devastating capability to create vast damage on both power systems and the society at large.**

Patterns of the blackout starting from the first triggering events to the system final status have emerged. A framework of a coding system was proposed in this paper in order to capture the common feature in the system evolution during the development of cascades. Cascades in a blackout can be tracked by a chain of events with the help of the codes. It is facile to adopt the framework to build up a knowledge base of blackouts.

By applying the proposed framework to 31 selected historic blackouts, most frequent events, effects and origins are identified; the findings can provide useful information for grid designers and security experts for ranking the most imminent issues in their study.

Index Terms **— Decision support systems, Pattern analysis, Network coding, Power system security, Risk analysis.**

I. Introduction

Power outage, also known as power cut, power failure, and blackout, is an impelling loss of the electric power supply to a large number of population over a wide geographical area for certain time. It is inevitably accompanied, especially in contemporary world, by huge economic costs and social impacts. Reference [1,2] discussed the socio-economic impact along with the impacts on the power system itself and on the society as a whole. Although, the resilience of system plan and operation makes blackouts comparatively rare in history, most power systems are only designed to sustain one or occasionally two independent equipment failures without cascading major outages to the customers.

Since the cost of blackouts are huge, non-stopping efforts have always been made to decrease the vulnerability of different layers of power systems, such as the physical layer, cyber layer, decision making layer, etc., so as to prevent economic and societal damage or at least to further reduce its possibility. However, all of these measures are costly. Therefore, there is need for panoramic understanding of how and where to allocate limited budgets for the preparedness of the system against potential failures or ceasing the development of the cascades in at a restrained level.

Many publications and technical reports have been made to analyze major power outages that had happened over time [3-16]. In those references, one can find detailed descriptions of the evolution of system failures and mechanisms leading to the blackout in study. The analyses of the individual blackout performed by those publications were very specific to the power outage in question; therefore, it is difficult to have a panoramic view on the most common chain of events that could lead to a major system failure.

Furthermore, research works from academia [17], industrial [18,19], and relative governmental agents [20, 21] consented that the tendency of blackouts would increase in the future due to many factors, such as intentional attacks (malicious threats), deteriorating global climate changes (natural threats), and lack of investment in the aging infrastructure (accidental threats and systematic threats), etc [17].

Therefore, the understanding of the common cascading mechanisms from triggering events to the final phenomena eventually causing blackouts is the most imperative step to prevent large scale blackouts, especially when the contemporary power systems are operated under extremely stressful conditions than ever before.

This paper tries to provide an overview of the chain of events than occur in the network after the materialization of a threat which created the triggering events leading to the final blackout by reviewing some important major historic power cuts. We introduced a new manner to describe the major outages around the world by employing a code system to form the chain. We analyzed 34 independent events among the most important 133 blackouts [17], which happened in the developed countries before 2000 and all over the world afterwards.

The rest of the paper is organized as follows: in section 2 the taxonomy used in the paper and the coding system are introduced. Section 3 presents the classification of threats, events, effects and phenomena used in the analysis of development of blackouts and their corresponding codes. Section 4 makes the statistic analysis by the framework set

This work was supported in part by the E.U. Commission under Grant Agreement 261696/2011 (SESAME project: https://www.sesame-project.eu/). The views expressed herein are those of the authors and can therefore in no way be taken to reflect the official position of the European Commission.

up in section 3. Section 5 provides some conclusive remarks.

II. Taxonomy

To avoid ambiguity the terms used in the paper are defined here. The definitions of the terms listed here only reflect what the paper refers to, not their replacement in some standards.

Threats: a source of danger indicating an imminent harm to power system. Threats in general can be classified into the following four categories [17, 22]:

- *Natural threats*: natural disasters not strictly controlled by humans which if occurring may impact the power system operation by causing damages (geomagnetic storms, earthquakes, forest fires, tsunamis, hurricane, flood, lightening, hail, animals, etc.);
- *Accidental threats*: failure of network devices and unintentional human decisional errors that may threaten the secure operation of the power system (operational fault, system equipment failure, accident due to the poor management, etc.);
- *Malicious threats:* intentional actions against power systems facilities and operation which are undertaken by different agents (terrorists, criminal groups, cyber attackers, copper theft, vandalism, psychotic attack, malware writer, etc.) and various means (explosives, high power rifles, malware, etc.) with the willingness to cause damage for political or economic benefits.
- *Emerging threats:* 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.

Events: topological changes of the physical system, loss of components function and variation of operation states because of an incident are defined as an event.

Effects: As the results of an event, power system' state in terms of electrical qualities will vary and get to a new state. This state shifting is defined as an effect.

Phenomenon: the main reason which directly or indirectly results in power supply failure and loss of load.

Failure: the state or condition of the power system in which a designed or intended objective cannot be met, including system blackout, power outage, transmission congestion, communicating media loss, etc.

Outage: a short or long term loss of the electric power to an area. It is a general item and the scale of an outage could be of any size.

Blackout: an accidental loss of electric power which would cause large economic losses and affect a large number of population and wide geographical area. It is the most severe situation of power outage.

Pre-condition: System operational conditions before the materialization of the origin of a blackout, including weather conditions, generation and load levels, significant scheduled outages, abnormalities and malfunctions of system components, including software.

Origin: the incident affecting one or more power system components which trigger a cascading failure. It is also used to indicate the first failure in the chain of events.

Chain of events: a sequence of undesired performance of system components, including malfunction, failure, damage, etc., which gives birth to and propagates the failure with respect to the ability to fulfil the purpose of the system.

Transient stability: the system's ability to maintain steady following a large disturbance [23] (system failure, loss of generation, or circuit contingences). As the disturbance here is lager, nonlinear differential equations must be used to describe the transient behaviors of some nonlinear dynamic components [24]. This is totally different from dynamic stability in which linear differential equations are used to describe the behaviors of all dynamic components.

Static stability: the system's ability to maintain steady following a small disturbance [23]. When modeling this problem the transient process of electromagnetic circuit should be neglected; the mechanical power is considered as constant, and the static characteristic of load is considered, thus the network can be represented by a set of algebraic equations.

Dynamic stability: system's ability to maintain steady following a small disturbance [23]. But the model of this problem is quite different from static stability. The dynamic characteristics of generator regulator and other components in the power system must be considered [25]. To describe this problem, both differential equations and algebraic equations should be used.

III. Framework of the Coding system

In order to focus on the evolution of each blackout and represent it in such a way that the cascading chain can be tracked by a sequence of codes, we set up a framework of a coding system containing detailed items and their corresponding codes to analyze the mechanism of blackouts. The framework could help us capture some patterns in the blackouts development.

One should notice the codes represented here are conceptual and based on the analysis of 31 different blackouts, selected according to their importance, impact magnitude, closeness to the contemporary power systems' situation and availability of technical reports. Therefore, it should be updated if items listed in Table I cannot reflect the specific feature of a blackout in study.

Each blackout, no matter where and when it happened, can be conceptually and distinctively divided into four parts: pre-condition, origin, chain of events and the end condition. In each of the four parts, several inferior categories can be determined as clusters of similar kinds.

Table I lists four groups of threats, events, effects and phenomena, in which the highlighted characters are employed to serve the purpose of coding the incident chain. It is expected to reproduce any major failure in power systems.

Example: A solar storm causes an overload in a transformer which then trips off the transformer, which then creates low voltage in the local area. Thus, using the code listed in the table, it can be represented as:

T-N-SPA-SOL/F-CUR-OVE/E-TRF-TR/F-VOL-LO

where the '/' signifies the word 'cause' or 'create', while '-' is used to represent the depth of an item in the table.

Example: the first term from above example "T-N-SPA-SOL" is the track of items that could be found in TABLE I

"SOL" (**Sol**ar flares) in "SPA" (**SPA**ce) subset of "N" (**N**atural threats) group under "T" (**T**hreats) column.

TABLE I. CLASSIFICATION OF THREATS, EVENTS AND EFFECTS IN POWER SYSTEMS

THREATS			**E**VENTS			**E**FFECTS		**P**HENOMENON
Natural threats	**GEO**logical disasters	**AVA**lanches	**GEN**eration Part	**GEN**erator	**TR**ip	**VOL**tage	**OV**er voltage	Voltage **C**ollapse
		EARthquakes						
		VOLcanic eruptions		**GEN**erator	**BR**eak		**LO**w voltage	
		LANdslides						
	HYDrological disasters	**FLO**ods		**BAC**kup generator	**FA**ilure		voltage **CO**llapse	
		LIMnic eruptions						
		TSUnamis		**TUR**bine	**MA**lfunction		**S**tatic voltage **S**tability	
	METeorological disasters	**BLI**zzards						
		ICE/hoar storm						
		COLd wave						
		CYClonic storms	transmission part [**TRS**]	transmission **LIN**e	**TR**ip		**D**ynamic voltage **S**tability	
		DROughts		**ISL**anding				
		HAIlstorms		transmission **LIN**e	**SH**ort circuit		**T**ransient voltage **S**tability	
		HEAt waves						
		TORnadoes		transmission **LIN**e	**BR**eak	**CUR**rent	**OV**er current	
		LIGhtning						
		THUnder		power **TOW**er	**CO**llapse	**ANG**le	**L**ow frequency **O**scillation	
		RAInstorm						
	FIRes	**WIL**d fires		**INS**ulators	**IN**sulation failure		**S**ubsynchronous **O**scillation*	
	HEAlth disasters	**EPI**demics		**BUS**bar	**MA**lfunction **SH**ort circuit			Stability **L**oss
		FAMines	transformation part [**TRF**]	**TRA**nsformer	**TR**ip		**S**tatic angle **S**tability	
	SPAce disasters	**IMP**act events						
		SOLar flares		**TRA**nsformer	**BR**eak		**D**ynamic angle **S**tability	
		GAMma ray burst		**SWI**tch	**MA**lfunction **SH**ort circuit			
				VOLtage control/ power **FAC**tor correction/ power **FLO**w control device	**MA**lfunction		**T**ransient angle **S**tability	
Accidental threats	**OPE**rational faults	**DES**ign error		lightning **ARR**ester	**MA**lfunction			
		WROng decision		circuit **BRE**aker	**MA**lfunction	**FRE**quency	**OV**er frequency	
		MAIntenance accident		**CUR**rent transformer	**MA**lfunction			
	EQUipments failures	**TEC**hnical failure		control and protective **REl**ay	**MAL**function		**LO**w frequency	
		ANImal interference						
		DEFective maintenance or maintenance error						
	FIRe threats	fire and **EXP**losion	**DIS**tribution Part	distribution **LIN**e	**TR**ip			
	NUClear threat	**NUC**lear disasters						
	HUMan threat	**OUT**sider threats						
		SOCial threats						
	CONtamination	**CHE**mical and biochemical contamination						
		SOLar flares/ solar winds / magnetic storms		distribution **LIN**e	**SH**ort circuit		**S**tatic frequency **S**tability	
Malicious threats	**PHY**sical threats	**TER**rorist attack		distribution **LIN**e	**BR**eak			
		WAR act		underground **CAB**le	**MA**lfunction		**D**ynamic frequency **S**tability	
		SABotage		**PO**le	**BR**eak			
	HUMan threats	**INS**ider threats		**FUS**e	**MA**lfunction		**T**ransient frequency **S**tability	
	CYBer threats	**MAL**ware	**INF**ormation , communication and control systems	cyber **EQU**ipment	**BR**eak			
		terrorists **HAC**king		cyber **SYS**tem	**HA**ck **MA**lfunction **BR**eak			

IV. Chain Of Events Analysis

In this section, we performed the statistical analysis on the chain of events using the code framework designed in the previous section to determine the sequence of events for some most typical blackouts, as shown in TABLE II. Table II contains the general information of blackouts in terms of their time and locations, threat types, triggering events and a part of chain of events of the evolution of the blackout, whereas Table III includes the rest of chain of events and the final phenomenon. It should be noted that the terms shown in parallel in the same cell signify the simultaneous occurrence of those incidents. Obviously, it is easy to quickly grasp how a specific blackout developed by reading the codes from TABLE II. Take the Brazilian blackout of November 2009 for example. The blackout was initiated by a rain storm as a natural threat ([T-N-MET-RAI]). The disturbance was reported to almost simultaneously start by some single phase short circuits in lines and a single phase short circuit on a busbar ([E-TRS-LIN-SH] and [E-TRS-BUS-SH]) [1]. As it is shown in TABLE II, these triggering events caused over current ([F-CUR-OV]) leading to the disconnection of some lines and tripping of some generator units (E-TRS-LIN-TR], [E-GEN-GEN-TR]). As a consequence of the over current conditions which triggered lines protection systems, there were some islanding synchronic with line disconnection event ([E-TRS-ISL]). Consequently, frequency increased up to 63.5 Hz in one island ([F-FRE-OV]) and decreased to 58.3 Hz in another one ([F-FRE-LO]). There were also overload and power swing as the effects of the later mentioned events ([F-CUR-OV], [F-ANG-SS]). All these disconnections caused a voltage collapse eventually, which is shown by [P-VC] as the phenomenon in Table III.

The new code system proposed in TABLE I enables the description and classification of the types of events or effects and the origins of blackouts. Based on the coding system, statistical results are illustrated in the following figures in order to capture the most common pattern of the evolution of blackouts. Generally, there were 17 types of events and 17 different kinds of effects based on the classification (TABLE I) in the studied cases. In the statistical analysis provided in this section, we mainly focused on the following three items: 1) frequency of appropriate events 2) the frequency of the appropriate effects and 3) the frequency of the origins of the blackouts.

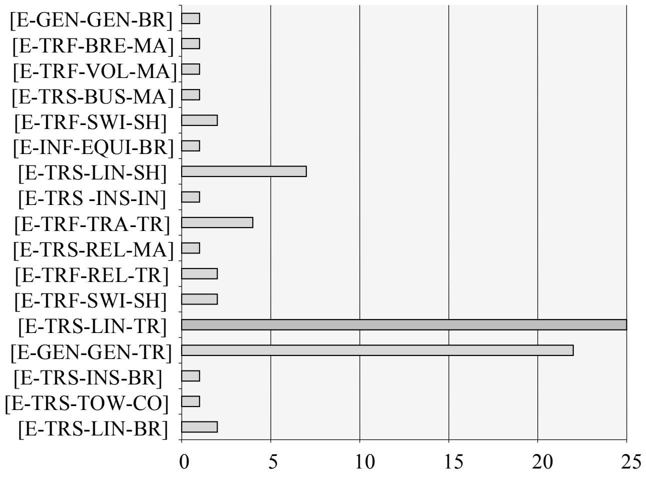

Figure 1. Occurrence of appropriate events in selected blackouts

Error! Reference source not found., provides the frequency of events based on the selected blackouts. For example [E-TRS-LIN-SH] which is the code for short circuit in transmission line as an event was found in 7 historic blackouts. Although the same event, like trip off a line, may happen in one blackout several times, which it would be better to count as several individual events; however as these details are not available for all the blackouts we selected; therefore, we only considered the same event one time in a specific blackout. It should be hence noted that the actual frequency of the most frequent events would be even higher than it is demonstrated here. For example, a transmission line trip is the most frequent event. According to our historic data analysis, a transmission line trip happened in 81% of the cases. The event of transmission line trip ([E-TRS-LIN-TR]) occurred 25 times shown in Figure 1 were observed in 80.64% of all the blackouts studied. In some cases like New York blackout in 1977 or Italy power outage experience in 1994, this event was observed in the chain of events report several times while in some blackouts such as Brazil blackout in 2002, there was only one reported in the cascading failure. In the both above mentioned cases, the event of transmission line trip was counted as one event. The counted events could be either as the origin of a blackout or a link in the chain during the power outage evolution.

As discussed in the previous section, each event leads to an effect or different effects depending on the context situation. But the frequency of each effect may rely on the vulnerabilities concerned. In Figure 2 the different historic blackouts which included the mentioned effect are illustrated as a bar chart.

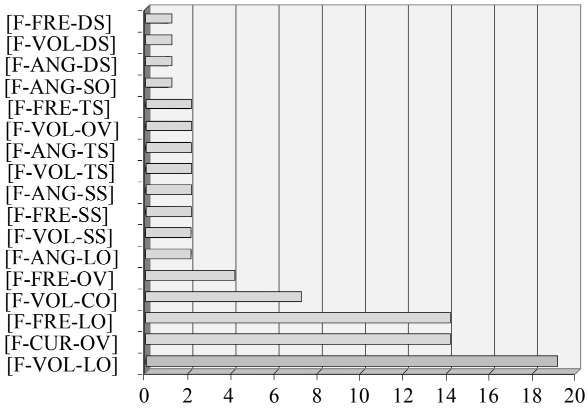

Figure 2. Occurrence of appropriate effects in selected blackouts

It is manifest from Figure 2 that low voltage was the most frequent effect in the evolution of all the selected blackouts, which was found in 19 cases among 31 studied cases. This signifies that low voltage has a 73% probability to happen at least once in each blackout. However, it should be noted that any kinds of effects might happen several times in each study case. According to the statistics, we can conclude that low voltage, over current and low frequency are the most typical and the most frequent effects which happened at least in half of the historic blackouts.

TABLE II. MOST TYPICAL CHAIN OF EVENTS

Location	Date	Threat	Chain of events					
Brazil	10/11/2009	[T–N–MET–RAI]	[E-TRS-LIN-SH] [E-TRS-BUS-SH]	[F-CUR-OV]	[E-TRS-LIN-TR] [E-GEN-GEN-TR] [E-TRS-ISL]			
Tennessee (USA)	22/08/1987	[T–N–MET–HEA]	[E-TRF-SWI-SH]	[F-VOL-LO]				
Western USA	10/8/1996	[T–N–MET–HEA]	[E-TRS-LIN-TR]	[F-CUR-OV] [F-VOL-LO]				
Western USA	2/7/1996	[T–N–MET–HEA]	[E-GEN-GEN-TR]	[F-ANG-DS] [F-VOL-LO]	[E-GEN-GEN-TR]	[F-VOL-LO]		
Poland	26/06/2006	[T–N–MET–HEA]	[E-GEN-GEN-TR]	[F-VOL-LO]				
New York	13/07/1977	[T–N–MET–LIG]	[E-TRS-LIN-TR]	[F-CUR-OV]	[E-TRS-LIN-TR] [E-TRS-REL-MAL]	[F-CUR-OV]	[E-TRS-LIN-TR] [E-TRF-TRA-TR]	[F-CUR-OV]
Canada	5/1/1998	[T–N–MET–ICE]	[E-TRS-LIN-BR]	[E-TRS-TOW-CO]				
France	26/12/1999	[T–N–MET–THU]	[E-TRS-LIN-TR]	[F-VOL-SS] [F-FRE-SS]	[E-GEN-GEN-TR]	[F-CUR-OV] [F-VOL-LO] [F-VOL-SS]		
Canada, Quebec	18/04/1988	[T–N–MET–TEC]	[E-TRS -INS-IN]	[E-TRS-LIN-TR]				
Italy	24/08/1994	[T–N–FIR–WIL]	Multiple [E-TRS-LIN-TR]					
England	28/08/2003	[T–A–OPE–DES]	[E-GEN-GEN-TR]					
Brazil	21/01/2002	[T–A–OPE–DES]	[E-TRS-LIN-TR]					
Malaysia	13/01/2005	[T–A–OPE–DES]	[E-TRS-LIN-TR]	[F-ANG-SS]				
USA-Canada	14/08/2003	[T–A–OPE _ WRO]	[E-TRS-LIN-SH]	[E-G-GEN-TR]	[F-CUR-OV] [F-VOL-LO	[E-INF-EQUI-BR]		
Northeast	19/09/1965	[T–A–OPE _ WRO]	[E-TRS-LIN-TR]	[F-CUR-OV]	[E-TRS-LIN-TR]	[F-CUR-OV] [F-ANG-SS]		
France	12/1/1987	[T–A–EQU–TEC]	[E-GEN-GEN- TR]	[F-VOL-LO]				
Tennessee (USA)	22/08/1987	[T–A–EQU–TEC]	[E-TRF-SWI-SH]	[F-VOL-LO]				
Italy	24/08/1984	[T–A–EQU–TEC]	[E-TRS-LIN-TR]					
Canada, Quebec	18/04/1988	[T–A–EQU–TEC]	[E-TRS-INS-IN] [E-TRS-LIN-SH]	[E-TRS-LIN-TR]				
Southern Sweden	23/09/2003	[T–A–EQU–TEC]	[E-GEN-GEN-TR]	[F-VOL-LO] [F-FRE-LO] [F-VOL-CO]	[E-TRS-BUS-MAL]			
Italy	28/09/2003	[T–A–EQU–TEC]	[E-TRS-LIN-SH] [E-TRS-LIN-TR] [E-TRF-TRA-TR]	[F-VOL-LO] [F-CUR-OV]	[E-TRS-LIN-SH] [E-TRS-LIN-TR] [E-TRS-LIN-TR]	[F-VOL-LO] [F-CUR-OV]		
Australia	13/08/2004	[T–A–EQU–TEC]	[E-TRS-LIN-TR]	[E-GEN-GEN-TR]	[F-FRE-LO]	[E-GEN-GEN-TR]	[F-FRE-LO]	
Western Norway	13/02/2004	[T–A–EQU–TEC]	[E-TRF-VOL-MAL]	[F-VOL-OV]				
Greece	12/7/2004	[T–A–EQU–TEC]	[E-GEN-GEN-TR]	[F-VOL-LO]	[E-GEN-GEN-TR]	[F-VOL-LO]		
Australia	14/03/2005	[T–A–EQU–TEC]	[E-TRS-LIN-SH]	[E-TRS-LIN-BR]				
Pakistan	24/09/2006	[T–A–EQU–TEC]	[E-TRF-TRA-TR] [E-GEN-GEN-TR]					
UCTE	4/11/2006	[T–A–EQU–TEC]	[E-TRS-LIN-TR] [E-GEN-GEN-TR]	[F-CUR-OV] [F-FRE-LO] [F-CUR-OV]	[F-CUR-OV]			
Spain	23/07/2007	[T–A–EQU–TEC]	[E-TRS-BUS-MA]	[E-TRS-BUS-MA]	[E-TRF-BRE-MA]			
Florida	26/02/2008	[T–A–EQU–TEC]	[E-TRS-LIN-SH]	[F-CUR-OC]	[F-VOL-TS]	[E-GEN-GEN-TR] [E-TRF-REL-MA]		
UK	27/05/2008	[T–A–EQU–TEC]	[E-TRS-LIN-TR]	[F-FRE-LO]	[E-TRS-LIN-TR]	[F-FRE-LO]	[E-TRS-LIN-TR]	
Vancouver	14/07/2008	[T–A–FIR–EXP]	[E-TRF-TRA-TR] [E-GEN-GEN-BR]	[F-VOL-LO]	[E-GEN-GEN-TR]			

TABLE II. MOST TYPICAL CHAIN OF EVENTS (CONTINUATION)

Location	Date	Chain of events						Phenomena
Brazil	10/11/2009	[F-FRE-OV] [F-FRE-LO] [F-CUR-OV] [F-ANG-SS]						[P-VC]
Tennessee (USA)	22/08/1987	Multiple [E-TRF-REL-TR] Multiple [E-TRS-LIN-TR] Multiple [E-GEN-GEN-TR]	[F-VOL-LO] [F-CUR-OV]					[P-VC]
Western USA	10/8/1996	[E-TRS-LIN-TR]	[F-ANG-SO] [F-FRE-LO]					[P-VC]
Western USA	2/7/1996	[E-TRS-LIN-TR]	[F-ANG-LO]	[E-TRS-LIN-TR]	[F-CUR-OV] [F-ANG-DS]			[P-VC] [P-SL]
Poland	26/06/2006	[E-TRS-LIN-TR]	[F-VOL-LO]					[P-VC]
New York	13/07/1977	[E-TRF-TRA-TR]	[F-CUR-OV]	[E-TRS-LIN-TR]	[F-FRE-LO] [F-VOL-SS]	[E-GEN-GEN-TR]	[F-FRE-SS] [F-ANG-SS]	[P-SL]
Canada	5/1/1998	[E-TRS-INS-BR]						[P-VC]
France	26/12/1999	[F-FRE-SS]	[F-CUR-OV]	[E-TRS-LIN-TR]	[F-VOL-CO]			[P-SL] [P-VC]
Canada, Quebec	18/04/1988	[F-FRE-LO]	[E-TRS-LIN-TR]					[P-VC]
Italy	24/08/1994	[F-CUR-OV] [F-FRE-LO]						[P-SL]
England	28/08/2003	[F-FRE-LO] [F-FRE-CO] [F-VLO-LO]						[P-VC]
Brazil	21/01/2002	[F-VOL-DS] [F-FRE-DS]						[P-SL]
Malaysia	13/01/2005	[E-TRS-ISL]	[F-VOL-LO] [F-FRE-LO] [F-FRE-OV]					[P-VC]
USA-Canada	14/08/2003	[E-TRS-LIN-TR]	F-CUR-OV F-VOL-LO	[E-DIS-LIN-TR] [E-TRS-LIN-TR]	[F-VOL-TS]	[E-TRS-LIN-TR] [E-TRS-LIN-TR]	[F-VOL-TS] [F-ANG-TS]	[P-SL]
Northeast	19/09/1965	[E-TRS-LIN-TR]	[F-CUR-OV] [F-ANG-TS]	[E-GEN-GEN-TR]	[F-ANG-TS] [F-FRE-TS]			
France	12/1/1987	[E-GEN-GEN-TR]	[F-VOL-LO]					[P-VC]
Tennessee (USA)	22/08/1987	[E-TRF-REL-TR] [E-TRS-LIN-TR] [E-GEN-GEN-TR]	[F-VOL-LO] [F-CUR-OV]					[P-VC]
Italy	24/08/1984	[F-CUR-OV] [F-FRE-LO]						[P-SL]
Canada, Quebec	18/04/1988	[F-FRE-LO]	[E-TRS-LIN-TR]					
Southern Sweden	23/09/2003	[E-GEN-GEN-TR] [E-TRS-LIN-TR]	[F-ANG-LO] [F-VOL-LO] [F-FRE-LO] [F-VOL-CO]	[E-TRS-LIN-TR]	[F-VOL-CO]			[P-VC]
Italy	28/09/2003	[E-TRS-LIN-TR]	[F-VOL-LO] [F-CUR-OV]					[P-SL] [P-VC]
			[F-FRE-LO]	[E-TRS-LIN-TR] [E-GEN-GEN-TR]	[F-FRE-LO] [F-FRE-OV] [F-VOL-OV] [F-VOL-CO]			
Australia	13/08/2004	[E-GEN-GEN-TR]	[F-FRE-LO]	[E-GEN-GEN-TR]	[F-FRE-LO]			
Western Norway	13/02/2004	[E- TRS-LIN-TR]	[F-CUR-OV] [F-VOL-OV] [F-VOL-CO]					[P-VC]
Greece	12/7/2004	[F-VOL-LO]	[E-GEN-GEN-TR]	[F-VOL-LO]				[P-VC]
Australia	14/03/2005	[F-CUR-OV]						[P-SL]
Pakistan	24/09/2006	[F-CUR-OV]						[P-VC]
UCTE	4/11/2006	[E-TRS-LIN-TR]	[F-CUR-OV]					[P-SL]
		[F-VOL-CO]						
		[E-GEN-GEN-TR]	[F-FRE-LO]					
Spain	23/07/2007	[E-TRS-LIN-TR]						
Florida	26/02/2008	[F-VOL-LO] [F-ANG-L-O]	[E-GEN-GEN-TR]	[F-FRE-LO] [F-FRE-OV] [F-FRE-TS]				
UK	27/05/2008	[F-FRE-LO]						
Vancouver	14/07/2008	[F-VOL-CO]						

Due to the same reason of counting each effect as we counted events, it should be noted that the real frequency of the 3 most frequent events would be actually higher than it is depicted here.

One of the most important concerns in terms of power systems vulnerabilities is illustrated in Figure 3. This figure shows the origins (triggering events) for all the blackouts we studied. When the initiating threat materialized, it started to generate a chain of events. Thus it is important to pay a special attention to the origin of the chain as it is triggering a phenomenon such as voltage collapse or stability loss which definitely creates the blackout.

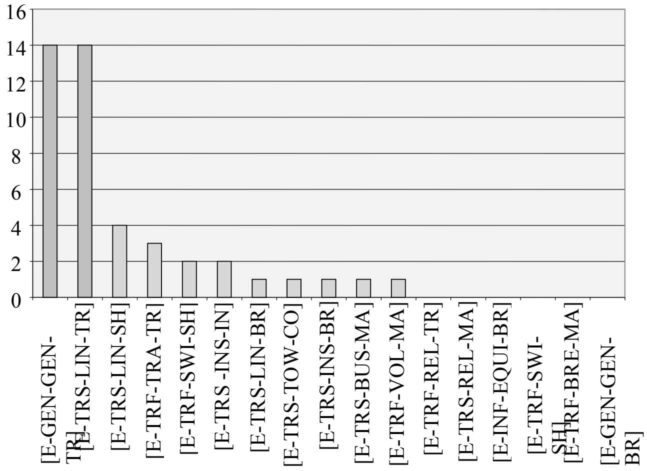

Figure 3. Occurrence of origins in the selected blackouts

According to the statistics, generator and transmission line trips ([E-GEN-GEN-TR] and [E-TRS-LIN-TR] respectively) are the most frequent origins (triggering events) that give birth to the whole blackout. As it is illustrated in Figure 3, both of the two events initiated 14 blackouts. It is manifest that these two events are more probable and important to the network planning and operation, compared with the rest of the events (more than three times in terms of their occurrence). In almost 90% of the studied cases, these two events triggered the cascading failures, which imply remarkable remedies to cease blackout if we can prevent such events happen at the very beginning.

According to the chain of events data in TABLE II, technical failure of equipments as accidental threats ([T-A-EQU-TEC]) was responsible for 50% of generator trip events as the origin of the cascades, and 40% of transmission line trip events which started the evolution of blackouts in studies.

For the most import threat, half of the studied blackouts happened due to technical failures, among which 33% caused generator trips and 33% incurred transmission line trips.

For the most crucial effect, 43% of the generator trips as the triggering events caused low voltage and 36% of transmission line trips as triggering events caused over current as the direct consequences, respectively, which are the most frequent physical effects in the studied blackouts evolutions as shown in Figure 2.

Besides the previously mentioned 2 most frequent effects, low system frequency can also be observed with the same occurrence as over current. From TABLE II, we can achieve that 48% of low voltages are caused by generator trips, 86% of over currents are due to transmission line trips, and 71% of under frequency happened due to generator and transmission line trips with more or less the same frequencies.

From the analysis of chain of events in the historic blackouts, it is obvious that the most important elements in the power system to enhance are the generators and transmission lines since no matter what threats happened to the power systems, that pieces of equipment would be the most vulnerable ones. In terms of the chain of events, the trip of generators and transmission lines are also the most frequent ones in the development of blackouts. It suggests that both the local protection scheme and equipment and global special protection schemes for generator and transmission lines need to be designed with special care.

V. Conclusion

During the past decades, power system blackouts have become more frequent than ever before. This increasing vulnerability is owed to exposure to various threats which generates a sequence of events in power systems that lead to a blackout [26]. Therefore, to have a better understanding of the common patterns on how an exterior factor could penetrate into power systems and create huge impacts on the society and economy, it is essential to set up a framework that allows us to quickly grasp the development of cascades in terms of chain of events that occurred in blackouts.

According to the analysis of the most typical sequence of events, it was determined that transmission line trips and generator trips are the most frequent events. The most frequent effect caused by different events is the low local voltage. Over current and low frequency are the next most frequent effects. The conclusion could help both grid designers and protection system engineers to rank the most imminent matters they are faced with. In addition, it could also be beneficial for security experts to rank the most severe threats to power systems by linking the threats and their origins and increase the levels of security for electricity infrastructures.

References

[1] Analysis of Historic Outages, SESAME Project - Securing the European Electricity Supply Against Malicious and accidental thrEats, Deliverable D1.1, Version: 2.0, 2011.

[2] T. Huang, A. A. Purcărea, S. L. Voronca, M. Cremenescu, Y. Wu, “General Overview on the Societal and Technical Impacts of Blackouts”, Acta Electrotehnica Special Issue Proceedings of the 5th International Conference of Modern Power Systems MPS 2013, 28 – 31 May 2013 Cluj Napoca, vol. 54, no. 5, pp. 219 - 225, 2013

[3] J. G. Calderon-Guizar, E. A. Tovar-Gonzalez, “Impact on Generator Reactive Power Limits on a Static Voltage Stability”, Advances in Electrical and Computer Engineering, vol. 11, no. 4, pp. 105-110, 2011. [Online]. Available: http://dx.doi.org/10.4316/AECE.2011.04017

[4] Z. Wang, Y. Zhang, J. Zhang, J. Ma, “Recent Research Progress in Fault Analysis of Complex Electric Power Systems”, Advances in Electrical and Computer Engineering, vol. 10, no. 1, pp. 28–33, 2010. [Online]. Available: http://dx.doi.org/10.4316/aece.2010.01005

[5] “Report on the blackout in Italy on 28 September 2003”, Swiss Federal Office of Energy (SFOE), 2003.

[6] J. Landstedt, P. Holmström, “Electric Power Systems Blackouts and the Rescue Services: the Case of Finland”, CIVPRO Working Paper 2007. [Online] Available: http://www.helsinki.fi/aleksanteri/civpro/publications/WP1.pdf

[7] O. Norio, T. Ye, Y. Kajitani, P. Shi, H. Tatano, “The 2011 Eastern Japan Great Earthquake Disaster: Overview and Comments”, International Journal of Disaster Risk Science, vol. 2, no. 1, pp. 34-42, 2011. [Online]. Available: http://dx.doi.org/10.1007/s13753-011-0004-9

[8] J. Watson, “Power Failure Leaves 5 Million in the Dark”, The San Francisco Chronicle, 2011. [Online]. Available: http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/09/08/MND01L2A1P.DTL

[9] “The Black-out in Southern Sweden and Eastern Denmark, September 23, 2003”, Final Report, Svenska Kraftnät, Vällingby, SWE, 2004

[10] R. Zimmerman, C. E. Restrepo, J. S. Simonoff, L. Lave, “Risk and Economic Costs of a Terrorist Attack on the Electric System”, Presentation for the CREATE Economics of Terrorism Symposium, 2005.

[11] K. B. McEachron, “Lightning - A Hazard to Electric Systems”, Power Apparatus and Systems, Part III, Transactions of the American Institute of Electrical Engineers, vol. 71, no. 1, pp. 977–982, 1952. [Online] Available: http://dx.doi.org/10.1109/AIEEPAS.1952.4498562

[12] V.D. Albertson, J.M. Thorson, R.E. Clayton, S.C. Tripathy, “Solar-Induced-Currents in Power Systems: Cause and Effects”, Power Apparatus and Systems, IEEE Transactions on, vol. PAS-92, no.2, pp. 471-477, 1973. [Online] Available: http://dx.doi.org/10.1109/TPAS.1973.293746

[13] E. Bompard, T. Huang, Y. Wu, M. Cremenescu, “Classification and Trend Analysis of Threats Origins to the Security of Power Systems”, International Journal of Electrical Power & Energy Systems, vol. 50, pp. 50-64, 2013. [Online] Available: http://www.sciencedirect.com/science/article/pii/S0142061513000689

[14] N. Dizdarevic, M. Majstrovic, J. Benovic, “Activation of Special Protection System During Blackout”, Proceedings of the 2004 Bulk Power System Control and Dynamics - VI, Cortina d'Ampezzo, It., pp. 22-27, 2004.

[15] G. Doorman et al., “Vulnerability of the Nordic Power System”, SINTEF Energy Research, Report to the Nordic Council of Ministers, 2004.

[16] H.F.Vosloo et al., The Susceptibility of 400 kV Transmission Lines to Bird Streamers and Bush Fires: A Definitive Case Study, 6th Southern Africa Regional CIGRE Conference, 2009.

[17] 2007 Long-Term Reliability Assessment, NERC (North American Electric Reliability Corporation), 2007, quotted in The NextGen Energy Council Management Information Services, Inc., “Lights Out in 2009? A Critical Analysis of the Threat of Major Blackouts Facing the U.S.; What Is Needed to Maintain Grid Reliability Through 2016, The Major Barriers to Keeping the Lights On”, 2008.

[18] K. Wheeler, Power Outage: Mixed Reactions from EG Residents. EastGreewichPath, 2011.

[19] P. Kundur, C. Taylor, “Blackout Experiences and Lessons, Best Practices for System Dynamic Performance and the Role of New Technologies”, IEEE-PES Special Publication 07TP190, Piscataway, NJ, 2007.

[20] G. Peters et al., “Transmission Line Reliability: Climate Change and Extreme Weather”, American Society of Civil Engineers, 2006.

[21] Global Climate Change Research, Forest Service United States Department of Agriculture. [Online]. Available: http://www.fs.fed.us/research/climate/

[22] Vulnerability and Threat Knowledge Base, SESAME Project - Securing the European Electricity Supply Against Malicious and accidental thrEats, Deliverable D1.2, Version: 1.0, 2012

[23] P. Kundur et al., “Definition and Classification of Power System Stability”, IEEE/CIGRE joint task force on stability terms and definitions Power Systems, IEEE Transactions on, vol. 19, no. 3, pp. 1387-1401, 2004. [Online] Available: http://dx.doi.org/10.1109/TPWRS.2004.825981

[24] B. M. Muthu, R. Veilumuthu, L. Ponnusamy, “An Effective Distributed Model for Power System Transient Stability Analysis”, Advances in Electrical and Computer Engineering, vol. 11, no. 3, pp. 71–76, 2011. [Online]. Available: http://dx.doi.org/10.4316/aece.2011.03012

[25] M. R. Banaei, A.-R. Kami, “Improvement of Dynamical Stability Using Interline Power Flow Controller”, Advances in Electrical and Computer Engineering, vol. 10, no. 1, pp. 42–49, 2010. [Online]. Available: http://dx.doi.org/10.4316/aece.2010.01007

[26] T. Huang, S. L., Voronca, A. A. Purcărea, A. Estebsari, “Challenges and Necessities of Vulnerability Assessment for Electricity Infrastructures", 5th International Symposium on Electrical Engineering and Energy Converters 2013, Buletinul AGIR nr. 4, pp. 19–22, 2013