Electrical Power and Energy Systems 81 (2016) 12–21

Contents lists available at ScienceDirect

Electrical Power and Energy Systems

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

A framework for analyzing cascading failure in large interconnected power systems: A post-contingency evolution simulator

Ettore Bompard [a], Abouzar Estebsari [a], Tao Huang [a,*], Gianluca Fulli [b]

[a] Dipartimento Energia, Politecnico di Torino, Torino 10129, Italy
[b] European Commission Joint Research Center, Institute for Energy and Transposrt, P.O. Box 2, NL-1755 ZG Petten, The Netherlands

ARTICLE INFO

Article history:
Received 22 December 2014
Received in revised form 15 January 2016
Accepted 9 February 2016

Keywords:
Power system security
Cascading failures
Countermeasure
Automatic restoration
Decision support

ABSTRACT

The power system protection against different threats has become a key and growing concern. A materialized threat provokes a sequence of chained events and counteractions in the grid. The simulation and analysis of the cascades leading to blackouts are extremely intricate due to various time scales, multiple interacting automatic and human-driving actions, and the large set of possible countermeasures. The possibility to simulate the cascading events, considering both behaviors of the system and human/automatic actions, is crucial for designing protective strategies, guiding investments and supporting policy decision making on reinforcing the system. In this paper, we present a simulation framework which, with a steady-state approach, provides system snapshots during cascading failures, taking into account the actions for minimizing the load-shedding or maximizing the restoration of the unserved loads. The conceptual framework is implemented as a software tool to simulate system behaviors and actions like automatic countermeasures, human interventions and optimal operational strategies to defend and restore the system. Combined with a suitable economic assessment method, it can be used to evaluate investments in countermeasures and the potential costs of different threats. It has been applied to study the countermeasures to enhance the security of the EU power transmission network.

Introduction

Infrastructures such as electric power, gas and oil networks, water networks, transportation networks, and telecommunication and computer systems are becoming increasingly interconnected with each other. This means that a threat to one infrastructure may rapidly create a global effect by cascading into other infrastructures [1].

Among all these infrastructures, electrical networks are becoming more and more critical, by themselves and for the operation of other infrastructures. Moreover, the growing interconnection and integration of variable generation sources has made the vulnerability of all other networks more dependent on electricity system security [2]. For example, in the 2003 Northeast Blackout, water pressure was lost due to lacked pumps power; all the trains running into and out of New York were shut down; cable television systems were out of order due to the loss of backup power; and cellular telecommunication was disrupted [3].

Today the electrical power systems on one hand are growing in complexity and vulnerability due to the amount of information exchanged, the new operational methods developed and the extensive use of smarter equipment. On the other hand, along with the traditional threats such as natural, accidental or malicious threats, new threats are emerging [4]. With large scale penetration of renewable energy sources (RES) into power grids, the transmission system faces more risks due to their intermittent nature, thus more attention is being paid on the development of transmission grid, striving to make it more intelligent and more suitable for the transmission of large energy quantities over far-away distances.

At least 20% of European energy has to be supplied by renewable sources by 2020 according to the recently adopted European renewable Directive 2009/28/EC. European electricity markets are expected to produce 30–35% by 2020 of its supplied energy by means of renewable resources such as wind and solar power, which are by their nature intermittent, less predictable and more geographically distributed [5–7].

Nowadays, the trial and adoption of innovative paradigms and technologies (such as distributed generation, smart grids and super grids) at infrastructural, operational, market and environmental level, along with fossil energy resources scarcity, energy demand

* Corresponding author. Tel.: +39 0110907117; fax: +39 0110907199.
E-mail addresses: ettore.bompard@polito.it (E. Bompard), abouzar.estebsari@polito.it (A. Estebsari), tao.huang@polito.it (T. Huang), Gianluca.Fulli@ec.europa.eu (G. Fulli).

http://dx.doi.org/10.1016/j.ijepes.2016.02.010
0142-0615/

increase, and energy market liberalization, seriously challenge power system security [8–12].

Security of electricity networks is one of the key objectives in the planning and operation and needs to consider the most credible threats to the power systems. In a single area such as a national power grid with a single transmission system operator, the security of the grid may not be as critical as a transcontinental network because in multi-area networks, like the ENTSO-E, neighboring grids may affect one another in case of facing abnormal situations. The evolution of a blackout may be controlled and even stopped in an area; however in the neighboring areas it may lead to severe problems [13]. Moreover, electricity exchange between different areas in a transcontinental network is increasing nowadays due to the increase of power trading. Such concerns make power system analysts paying more attention to the system security [13].

In order to prevent catastrophically unexpected effects to various aspects such as society, economy and industry, power system cascading failures have been studied more seriously in the recent years to urge engineers and scientists to pay more attention to the reasons of power outage. Many investigations have already indicated that cascading failure is one of the main reasons of blackouts [1,14–20]. Identifying the chain of events and finding out how they combine into cascading sequences is getting challenging nowadays [4,21,22,25,27,28].

As the conventional power system security analysis methods are mainly based on multiple case studies with a limited prediction of operational states, cascading failures in the interconnected power system operations can cause large-scaled blackouts. Moreover, most of the existing methods evaluate the consequences for a given contingency considering only one of the phenomena, and it has always been difficult to model and analyze successive combinations of the phenomena. Current standard stability analysis tools such as TRELSS [23], Static Security Assessment programs [24], Transient Security Assessment tools [25,29], Voltage Security Assessment programs [30,31] or Small Signal Analysis programs [32,33] usually focus on the electrical phenomena and often do not model protection in spite of the fact that protections in blackout are crucial [34]. In practice, the operation of the power system reacts to the incidents based on lessons and experiences learned from similar blackouts or simulation results from that non-comprehensive software. Existing tools to simulate system status can only cover a limited set of contingencies. Therefore, it is imperative to have a simulation tool which can not only reproduce the blackout but also predict the chain of events of a blackout *before* it happens as well as derive the best restoration strategies if necessary. Therefore, power systems modeling and planning requires advancement of the conventional security analysis methods [35,36].

Considering load curve, switching actions, time-based automatic operations and human interventions, power system operational conditions change over time; however the present protective systems and invested countermeasures are all designed without adapting to these changes. Even in the offline studies, it is still challenging to find out when and under what situations they should react how.

In this paper, we introduce a conceptual framework, implemented in a software tool, to simulate the evolution of failures in a power system along with modeling a large set of current automatic remedy actions and optimal operational human decisions. Besides, operative strategies based on the expertise of the user can be applied through the human intervention interface; it can also be used to simulate human errors during the blackout development.

The remainder of this paper is organized as follows. In Section 'A framework for the simulation of post-contingency evolution', the conceptual framework is introduced along with the main objectives and its components. In Section 'Structure of post-contingency evolution simulator', the structure of the framework, including the modules such as scheduler, automatic measures and optimal operation decision, and functions are presented. In S ection 'Application of PCES', an application of the proposed framework for power system security reinforcement is discussed. In Section 'Case study' we demonstrate an illustrative case based on the IEEE 30-bus system to demonstrate the validity of the concept and related software. Conclusive remarks are given in Section 'Conclusion'.

A framework for the simulation of post-contingency evolution

In this section, we briefly introduce the designed simulation framework, its key components and the conceptual considerations. We developed a framework named Post Contingency Evolution Simulator (PCES) to chronologically simulate the sequence of post-contingency failures ("cascading failure") and the restoration actions over time, under simplified hypothesis that the evolution of the network can be modeled as a sequence of equilibrium derived from a steady-state model of the system, which besides the common simplified conceptual elements (generators, branches, loads), also includes capacitor and shunt inductor banks, FACTS devices and DC lines, phase shifters, and pumped-storage stations. Hence the framework can be used to check the existence of a new equilibrium point, after a series of events, considering both decisions from automatons, e.g. protections, automatic controllers, etc., and from humans modeled as optimal decision making in terms of minimizing the load shedding or maximizing load pick up.

We consider the system power-frequency characteristic for the entire system, including generator droop and load frequency response, under a simplified steady-state approach when applying system frequency control. In case of islanding, the power-frequency characteristics are dynamically assigned to each island.

The first set of actions of the system during the evolution of a contingency represents the "*first-stage reaction*" which implements automatic responses (component-wise protection relays, system voltage controllers, frequency control system), and time-based human interventions (changing the status or settings of generators, pumped-storage stations, transformers, protections, FACTS, etc). If this reaction cannot lead to a new equilibrium or the new equilibrium implies a loss of load with respect to the load curve, a "*second-stage reaction*" is undertaken. This reaction is aimed at minimizing the load shedding and accelerating the load restoration resorting to a set of strategies, in which loads are kept as much as possible according to different levels of priority and their possible contributions to the acceleration of system restoration.

An extended network model is provided as an input in terms of network topology and parameters, protection settings, restoration time (specifying after how long an element can be put into use again), and the related restoration cost. Additional inputs include load curve, a set of countermeasures and simulation parameters (second-stage reaction initiating time, simulation end-time, etc.).

The evolution of the system is initiated by a triggering event that can be selected from a list of contingencies. Triggering events represent the materialization of one or more threats [25,26]. For example, a flood as an instance of a natural threat may destroy some buses, disconnect some lines and trip some generators in the physical layer.

As shown in Fig. 2, after the triggering event occurs, the system automatically reacts to the failures by means of protection relays and automatic control units. This process also involves some actions applied by time-based human interventions.