Vulnerability Assessment Scheme for Power System Transmission Networks Based on the Fault Chain Theory

Ansi Wang, Yi Luo, Guangyu Tu, and Pei Liu

***Abstract*—Vulnerable transmission lines or sections have great impacts on large-scale blackouts and cascading failures in power grids. A comprehensive scheme to study transmission vulnerability based on the fault chain theory of security science is proposed in this paper. In this scheme, the cascading failure process and its generic features are described according to a fault chain. Power flow transfer, sequent overload of lines, and damage of transmission sections are modeled and normalized to predict all the fault chains. On the basis of the fault chains, a new vulnerability assessment index is presented to identify critical lines and sections contributing to failure extension and system instability. The effectiveness of the proposed assessment scheme is demonstrated via numerical examples on three power systems. Considering operation properties and transient impact, the proposed scheme can be executed in an efficient way.**

***Index Terms*—Cascading failures, failure extension, fault chain theory, large-scale blackouts, system instability, vulnerability assessment index.**

I. Introduction

SEVERAL cascading failures and blackouts in power systems occurring in recent years [1], [2] highlight the need for vulnerability assessment. Large-scale blackouts which present severe threats to the society typically become widespread due to a complicated sequence of cascading failures [3]. The vulnerable transmission segments of power systems play an important role during the course of failure extension. The transmission vulnerability is a measure of the weakness and the incidence of lines or sections with respect to cascading events. Identifying these vulnerable lines or sections, and studying the vulnerability degree of transmission network are the necessary precondition for monitoring and security control of power systems.

Vulnerability assessment is the challenge of modeling the cascading failure and determining the vulnerability degree. Two main modeling methods have been developed to evaluate the vulnerability of transmission networks. The first is the topological complex network method describing cascading failures without taking into account the power flow. A model based on the small-world network has been proposed to identify the vulnerable lines [4]. A topological approach according to transmission efficiency was designed to analyze structural vulnerability of power grids [5], [6]. These topological metrics such as degree distribution, betweenness centrality, and network efficiency can approach the vulnerability problem from a more general perspective [7]–[10]. However, electrical quantities and power flow constraints are not considered for modeling cascading failure in these topological assessment methods.

Secondly, in the case of slow migration from one steady state to another, cascading overload and disconnection of transmission lines can be described by power system steady-state models [11], [12]. Some vulnerability assessment methods using steady-state model ignored the transient process and system stability so that they cannot represent the system behavior accurately [13]. Based on a steady-state model, vulnerability assessment can be performed by n-k contingency analysis [14], [15], which would consume large amount of computational time [16]. Therefore, an important problem is how to identify the credible n-k contingencies and apply high-performance computing techniques to check a maximum number of contingencies within time constraint [17]. The contingency screening, proposed in [18] and [19], can detect the fewest lines resulting in a failure of specified severity and identify severe multiple contingencies by detailed n-k analysis. This approach can provide an avenue to undertake a higher order n-k security analysis without vast combinatorial problem.

Additionally, the vulnerability assessment of power systems due to intentional outages has received significant attention by some researchers [20]. Salmeron *et al.* [21] were the first to formulate the terrorist threat problem as a max-min problem. The general bilevel programming framework, defining different objective functions for the terrorist and the operators, has been employed to identify the critical vulnerabilities by Arroyo *et al.* [22]. The bilevel programming techniques appear promising at identifying the potential target for terrorist agents. The intentional attack vulnerability analysis aims at identifying critical component set, which is evaluated by load shedding amount. The ultimate goal is to harden the critical components against intentional attacks.

The aim of this paper is to identify the critical events contributing to widespread cascading and instability under random

Manuscript received October 28, 2009; revised January 23, 2010 and April 01, 2010; accepted May 26, 2010. Date of publication July 12, 2010; date of current version January 21, 2011. This work was supported in part by the Program for Risk Assessment of Large Scale Grid Security, the State Grid Company of China (SGKJJSKF [2008]469). Paper no. TPWRS-00848-2009.

The authors are with Electric Power Security and High Efficiency Key Lab, Department of Electrical Engineering, Huazhong University of Science and Technology (HUST), WuHan 430074, China (e-mail: Ansi.Wang@hotmail.com; luoyee@mail.hust.edu.cn; gytu@public.wh.hb.cn; sunpei@public.wh.hb.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TPWRS.2010.2052291

or intentional attacks, and the ultimate goal is to prevent the large-scale blackout by online monitoring and security control.

This paper addresses the problem of vulnerability assessment through two stages: 1) developing a fault-chain-theoretic model of cascading outage; 2) determining the vulnerability degree for lines or sections.

Power system fault-chain-theoretic model is developed from the Heinrich's Domino Model of Accident Causation [23]. The proposed model describes the cascading failure as a kind of domino effect. It indicates that each event of the cascading failure is always dependent on other events. Therefore, the cascading blackout is a result of a series of events occurring step by step. The first contribution in this paper rests with proposing a prediction approach with a normalized index for obtaining fault chains online. The advantages of the approach are that: 1) the operational parameters and system stability can be taken into account for the assessment; 2) the contingency enumeration which enumerates all possible contingencies resulting in system instability can be avoided in large-scale power systems.

By exploiting similarities between the operational security and the reliability, the system fault chains can be regarded as the minimal cut-sets of the fault tree if the top event is a system blackout. An additional contribution in this paper is to convert the vulnerability analysis problem of the transmission network into an importance measure problem of the fault tree. The importance measures available can be categorized in two ways: probabilistic (such as the Birnbaum's measure and the criticality importance factor) and deterministic (such as the structural importance measure) [24]–[26]. As the work is concerned about the structural importance of lines, the former depending on each component's probability of a failure is not suitable for large-scale power systems. The latter assessing the importance in terms of the position in the tree can address the ordering issue efficiently. But it ignores occurrence probabilities of fault chains and the importance of a segment in different fault chains. So a new vulnerability index derived from the structural importance measure is proposed to overcome the drawbacks.

The validity of the proposed fault-chain-based analysis scheme is observed by virtue of the tests on a three-bus system, the IEEE 14-bus power system, and the Central Grid of China. It is observed that the proposed approach can capture network operational properties and be implemented in an efficient way.

The remainder of this paper is organized as follows. In Section II, the concept and the identification method of the fault chain are presented. In Section III, the vulnerability index and assessment procedure are developed. Section IV provides numerical results to illustrate the performance of the proposed scheme. In Section V, relevant conclusions are drawn.

II. Power System Fault Chains

A. Fault Chains and Cascading Failures

Cascading failures are the main way that blackouts become widespread [27], [28]. The cascading failure possibly results from a lot of reasons such as operational conditions, management, and human factors, which objectively exist in the network from the point view of fault chain theory. The reasons are the influencing factors of the fault chain associated with all the nodes and lines.

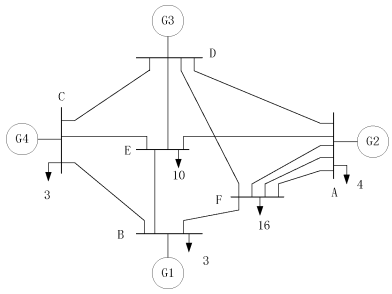

Fig. 1. Example system.

For instance, the occurrence process of the cascading failure and the blackout can be illustrated by the example system shown in Fig. 1.

The relay protections of the system are equipped normally. Suppose that one of the lines between bus A and bus F is repaired, and another line of the A-F transmission section is switched off by the main protection due to a single-phase short-circuited fault. The only tie line of the A-F transmission section would be overloaded and then disconnected because the control equipments are not carefully cooperated with overload protection and low-voltage load-shedding in terms of action time. As a consequence, the A-F transmission section is disconnected completely and the load of bus F is transferred; then lines B-F and D-F would be overloaded one after another. Cascading failure would occur once the corresponding relay protections operate.

The process of the contingencies can be described by the fault chain, which includes top event and basic events [29]. Let basic events of the three lines of A-F sections be b1, b2, and b3, and the basic events of the lines of sections B-F and D-F are b4 and b5, respectively. The top event, that is, the system blackout, is noted as $\boldsymbol{S}$. Then, a fault chain can be expressed as

$$\boldsymbol{S} : \overrightarrow{L}\, i = \{b1, b2, b3, b4, b5\} \tag{1}$$

where, $\overrightarrow{L}\, i$ is the ith fault chain of the example. Basic events b1, b2, b3, b4, and b5 result in the top event $\boldsymbol{S}$ all together, and each basic event occurs when the previous basic events have occurred. Thereby, the following characteristics of a cascading failure can be described by the fault chain.

1) Large-scale blackout is a small probability event.
2) The system is more dangerous when the number of the segments of a fault chain is increased.
3) The system would be unstable if a fault chain is triggered.
4) The segments of a fault chain are associated with power flow transferring.

The fault chain is applied to modeling the cascading failure. The segments of a fault chain should be determined at first. In the conventional fault-tree analysis [29], the minimal cut-set of a fault tree was dependent upon the way how the fault tree is formed. Therefore, fault chains regarded as minimal cut-sets can be obtained offline based on the conventional fault tree, which