Available online at www.sciencedirect.com

ScienceDirect

Electric Power Systems Research 77 (2007) 1132–1142

ELECTRIC POWER SYSTEMS RESEARCH

www.elsevier.com/locate/epsr

A new analysis method for early detection and prevention of cascading events

Hongbiao Song*, Mladen Kezunovic

Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX 77843-3128, USA

Received 8 May 2006; received in revised form 18 September 2006; accepted 19 September 2006
Available online 7 November 2006

Abstract

This paper introduces a new analysis method for early detection and prevention of power system cascading events. It uses the vulnerability index (VI) and margin index (MI) to evaluate the vulnerability and security of the individual system parts, as well as the whole system during an operating state. It identifies the vulnerable parts of the power system using the topology processing and operation index methods. For a given disturbance, it calculates the power flow, evaluates the vulnerability and security, identifies the vulnerable part, finds the transmission line overload and bus voltage problems, and predicts the possible successive events. The approach defines the control means using the following methods for early detection and prevention of cascading events: network contribution factor (NCF), generator distribution factor (GDF), load distribution factor (LDF), and selected minimum load shedding (SMLS). This approach has been tested using the IEEE RTS-96 24-bus system and promising results have been obtained. The proposed approach allows the power system operator to detect initial stages of cascading events and assert actions that will prevent such events from unfolding.

Keywords: Cascading events; Power system; Vulnerability; Security analysis; Load shedding; Large area blackout

1. Introduction

Power system cascading event is quite often a very complex phenomenon with low probability of occurrence but potentially catastrophic social and economical impacts. There are many cascading events resulting in large area blackouts worldwide, such as, 1965 US-Northeastern blackout, 1977 US-New York blackout, 1978 France blackout, 1996 US-Western blackouts, 2003 US-Northeastern blackout, 2003 Italy blackout, 2005 Russia-Moscow blackout, etc. [1–7]. Variety of research efforts are aimed at understanding and finding ways to prevent or mitigate cascading events: study of the cascade model, dynamic decision-event tree analysis, wide area backup protection, relay hidden failure analysis, special protection scheme, self-healing system with the aid of multi-agent technology, etc. [8–12]. The mentioned techniques are still far from being an established practice in solving the cascading event problem.

In general, cascading event is not a sudden event that human being cannot prevent or mitigate. Normally there are two stages of a cascading event [13]. First, there is a period of slowly evolving successive events that can be approximated with steady state analysis. The system operating conditions may get worse with several new disturbances following one another. Second, after succession of several major disturbances, there is a fast transient process resulting in cascading events and finally the system collapses. When the total system collapse starts, normally it is too late to stop it. However, much can be done during the slow steady state successions at the fist stage.

Early proper control actions at the steady state stage can prevent the possible cascading event. For example, on 3 July 1996, the Western Coast system operators manually shed load to avoid the possible cascading event when conditions were similar to 2 July [4]. On 26 August and 30 October 1996, the appropriate steady state control by system operators of New York Power Pool prevented the possible cascading event if the next worst contingency had occurred [4]. One thousand and five hundred mega Watts load shedding within Cleveland-Akron area before the tripping of Sammis-Star line could have prevented the blackout [5].

* Corresponding author. Tel.: +1 979 847 9069; fax: +1 979 845 9887.
E-mail addresses: songjefferson@neo.tamu.edu (H. Song), kezunov@ece.tamu.edu (M. Kezunovic).

0378-7796/$ – see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.epsr.2006.09.010

Steady state method was used successfully to simulate the cascading sequence of 2003 US-Northeastern blackout using rough information [14]. It was also used by the task force to benchmark the pre-cascade conditions of the Northeastern power system and conclude that the system was secure at 15:05EDT before the loss of Harding-Chamberlin line [5]. A similar method was used to simulate terrorist attack plan to find the vulnerability of the system [15].

This paper aims at early detection and prevention of cascading event using steady state analysis method at its initial steady state stage. This method can be implemented to work automatically with or without operator supervision, and can serve as a decision-support tool for real time operation or operator training purpose.

The framework of the proposed method is as follows. First, the power system is monitored to see whether there are any events or changing conditions during the system normal operation. Second, the system conditions are evaluated by computing the vulnerability index and margin index. Those indices can give specific quantitative measure of system vulnerability and security margin. Third, if the system is determined to be secure (not vulnerable), the monitoring of the system continues. Otherwise, the vulnerable parts of the system and vulnerable conditions are identified, the possible voltage and overload problems if those vulnerable conditions occur are predicted, the suitable control means to prevent or mitigate the problems are identified, and the control means are activated when needed.

Section 2 presents the comprehensive vulnerability index and margin index to evaluate the power system operation. Section 3 gives methods of topology processing and operation index to identify the vulnerable parts of the power system. Section 4 introduces the fast network contribution factor (NCF) method and uses it to predict the line overload and bus voltage problems for a given network event or assumed contingency. Section 5 provides the steady state control scheme based on network contribution factor (NCF), generator distribution factor (GDF), load distribution factor (LDF), and selected minimum load shedding (SMLS) methods to prevent and mitigate possible cascading event. Section 6 presents the study results. Section 7 concludes the paper.

2. Evaluation of the power system operation

Power system operators need to know as precisely as possible the security condition of the system operation. Thus they can take some control actions when the system security is being or has been threatened.

Security of a power system refers to the degree of risk in its ability to survive imminent disturbances (contingencies) without interruption of customer service. Stability of a power system refers to the continuance of intact operation following a disturbance [16]. Vulnerability can be taken as a measure opposite to security. The system is vulnerable if contingencies lead to an interruption of service to a part or the entire system. The element is vulnerable if contingencies or changing conditions lead to violation of the element limit, outage or mal-function of the element.

Before the power system faces interruption of service or the element faces outage or mal-function, some indices can be used to represent the degree of vulnerability and security. Vulnerability index (VI) and margin index (MI) are proposed to represent comprehensive and quantitative vulnerability and security information of the individual part and whole system [17]. Given a system with m generators, n buses, p lines and q loads, we define the vulnerability index (VI) and margin index (MI) sets as follows

A. Vulnerability index and margin index for generators:

$$\mathrm{VI}_{\mathrm{Pg},i} = \frac{W_{\mathrm{Pg},i}}{2N}\left(\frac{\mathrm{Pg}_i}{\mathrm{Pg}_{i,\max}}\right)^{2N}, \tag{1}$$

$$\mathrm{VI}_{\mathrm{Qg},i} = \frac{W_{\mathrm{Qg},i}}{2N}\left(\frac{\mathrm{Qg}_i}{\mathrm{Qg}_{i,\max}}\right)^{2N}, \tag{2}$$

$$\mathrm{VI}_{\mathrm{gen\_loss},i} = W_{\mathrm{gen\_loss},i}k_{\mathrm{gen\_loss},i}, \tag{3}$$

$$\mathrm{VI}_{\mathrm{gen}} = \sum_{i=1}^{m}(\mathrm{VI}_{\mathrm{Pg},i} + \mathrm{VI}_{\mathrm{Qg},i} + \mathrm{VI}_{\mathrm{gen\_loss},i}), \tag{4}$$

$$\mathrm{MI}_{\mathrm{Pg},i} = 1 - \frac{\mathrm{Pg}_i}{\mathrm{Pg}_{i,\max}}, \tag{5}$$

$$\mathrm{MI}_{\mathrm{Qg},i} = 1 - \frac{\mathrm{Qg}_i}{\mathrm{Qg}_{i,\max}}. \tag{6}$$

B. Vulnerability index and margin index for buses:

$$\mathrm{VI}_{V,i} = \frac{W_{V,i}}{2N}\left(\frac{V_i - V_i^{\mathrm{sche}}}{\Delta V_{i,\mathrm{lim}}}\right)^{2N}, \tag{7}$$

$$\mathrm{VI}_{\mathrm{Loadab},i} = \frac{W_{\mathrm{Loadab},i}}{2N}(r_{\mathrm{Loadab},i})^{2N}, \tag{8}$$

$$\mathrm{VI}_{\mathrm{load\_loss},i} = W_{\mathrm{load\_loss},i}k_{\mathrm{load\_loss},i}, \tag{9}$$

$$\mathrm{VI}_{\mathrm{bus}} = \sum_{i=1}^{n}(\mathrm{VI}_{V,i} + \mathrm{VI}_{\mathrm{Loadab},i} + \mathrm{VI}_{\mathrm{load\_loss},i}), \tag{10}$$

$$\mathrm{MI}_{V,i} = 1 - \left|\frac{V_i - V_i^{\mathrm{sche}}}{\Delta V_{i,\mathrm{lim}}}\right|, \tag{11}$$

$$\mathrm{MI}_{\mathrm{Loadab},i} = 1 - r_{\mathrm{Loadab},i}. \tag{12}$$

C. Vulnerability index and margin index for branches:

$$\mathrm{VI}_{\mathrm{Pf},i} = \frac{W_{\mathrm{Pf},i}}{2N}\left(\frac{\mathrm{Pf}_i}{S_{i,\max}}\right)^{2N}, \tag{13}$$

$$\mathrm{VI}_{\mathrm{Qf},i} = \frac{W_{\mathrm{Qf},i}}{2N}\left(\frac{\mathrm{Qf}_i}{S_{i,\max}}\right)^{2N}, \tag{14}$$

$$\mathrm{VI}_{\mathrm{Qc},i} = \frac{W_{\mathrm{Qc},i}}{2N}\left(\frac{\mathrm{Qc}_i}{Q_{\Sigma}}\right)^{2N}, \tag{15}$$

$$\mathrm{VI}_{\mathrm{line\_ang},i} = \frac{W_{\mathrm{line\_ang},i}}{2N}\left(\frac{\mathrm{La}_i}{\mathrm{La}_{i,\max}}\right)^{2N}, \tag{16}$$