Jie Yan
Ph.D.
Electrical Engineering

A new emergency control method and a preventive mechanism against cascaded events to avoid large-scale blackouts

Abstract

Cascaded events may cause a major blackout which will lead to a massive economic loss and even fatalities. Lots of research efforts have been made to address the issue systematically: preventive mechanisms are designed to mitigate the impact of initiating events on the power systems; emergency control methods are proposed to prevent the power systems entering an unstable state; restorative control methods are developed to stop the propagation of power system instability and to prevent large-scale blackouts.

This work contributes to the development of new emergency control methods and preventive mechanisms.

Firstly, a new emergency control scheme is proposed for preventing the power systems from loss of synchronism. Traditional out-of-step relays fail to predict loss of synchronism as the dynamics of the power systems become more and more complex. In recent years, the installation of Phasor Measurement Units (PMUs) on the power grids has increased significantly and, therefore, a large amount of real-time data is available for on-line monitoring of the power system dynamics. This research proposes a PMU-based application for on-line monitoring of rotor angle stability. Lyapunov Exponents are used to predict loss of synchronism. The relationship between rotor angle stability and the Maximal Lyapunov Exponent (MLE) is established. A computational algorithm is developed for the calculation of the MLE in an operational environment. The effectiveness of the monitoring scheme is illustrated with a 3-machine system and a 200-bus system model.

Secondly, a preventive mechanism against cyber attacks is developed. Cyber threats are real for the power systems. For example, hackers may attack the power control systems via the interconnected enterprise networks. This research proposes a risk assessment framework to enhance the resilience of the power systems to cyber attacks. Duality Element Relative Fuzzy Evaluation Method (DERFEM) is employed to evaluate the identified security vulnerabilities within the cyber systems of the power systems quantitatively; Attack Graph is used to identify the possible intrusion scenarios that exploit multiple vulnerabilities; an Intrusion Response system (IRS) is developed to monitor the impact of the intrusion scenarios on the power system dynamics in real time. The IRS calculates Conditional Lyapunov Exponents (CLEs) on line based on PMU data. Power system stability is then predicted through the values of the CLEs. Control actions based on the CLEs will be suggested if power system instability is deemed to happen. A generic wind farm control system is used for the case study. The effectiveness of the IRS is illustrated with the IEEE 39 bus system model.