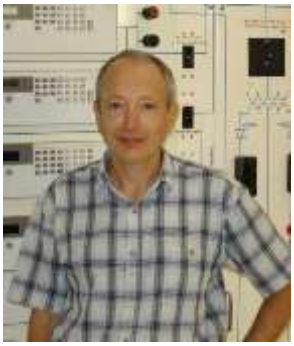
High Renewable Energy Penetration and Power System Security: New Challenges and Opportunities

Professor Michael Negnevitsky, University of Tasmania, Australia

Abstract

The word “security” in the context of a power system implies its security against a complete collapse, or a blackout. Secure operation involves practices aimed to keep the system operating normally when contingencies occur. An increasing penetration of intermittent renewable energy generation introduces additional uncertainties in power systems. However, the impact of variable generation on the system security is often exaggerated. On average, no significant mitigation measures are required until the wind and solar penetration reaches 20 per cent. The main challenge facing a power system with high penetration of renewables is the displacement of conventional synchronous generation by non-synchronous generation. Kinetic energy stored in the rotating masses of synchronous generators provides the system rotational inertia. Wind power generators are mostly doubly-fed induction or full-converter machines. Because these machines are either partially or completely decoupled from the grid by electronic converters, they do not provide inertia to the system. This reduces the total system inertia, and as a result, the system becomes more vulnerable to contingencies. Traditionally security assessment is performed based on deterministic criteria. The *N*-1 security criterion requires a power system to withstand an outage of any single system component without violating any system operating limits. This is based on the worst-case scenario criterion and provides a simple rule in the system design and operation. It has satisfied the needs of the power industry for decades. However, the deterministic approach to security is not adequate in modern power systems with market driven dispatch and high penetration of renewable energy and distributed generation. In this paper, security is defined as the risk in the system’s ability to withstand random contingencies without interruption to customer service. The higher the risk the lower the security, and vice-versa. System operational risk is defined as the sum of products of the probabilities of random contingencies that may occur in a particular system state and the expected cost of load interruptions caused by these contingencies. In calculating the operational risk, we take into account not just the likelihood of contingencies, but also uncertainties in load variability and renewable energy generation. In risk-based security assessment, we generate contingencies at random, based on their probabilities. Then, we assess the consequences of these contingencies in order to determine whether loads are disconnected following voltage violations, overloads and significant imbalance between load and generation.

Bio



Professor Michael Negnevitsky is Chair in Power Engineering and Computational Intelligence and Director of the Centre for Renewable Energy and Power Systems, University of Tasmania, Australia. The primary focus of his research is smart grids, power system security, demand response, and isolated and remote area power systems with high renewable energy penetration. Professor Negnevitsky authorised more than 400 research publications including 102 journal papers, more than 300 conference papers, 12 chapters in books, 2 books, 9 edited conference proceedings and received 4 patents for inventions. He is Fellow of Engineers Australia, and Member of the National ITEE College Board. Professor Negnevitsky is Chair of the IEEE PES Working Group on High Renewable Energy Penetration in Remote and Isolated Power Systems, Vice Chair of the IEEE PES Working Group on Asian and Australasian Infrastructure – Smart Grids with Large Penetration of Renewable Energy, Member of CIGRE AP C4 (System Technical Performance) and CIGRE AP C6 (Distribution Systems and Dispersed Generation), Australian Technical Committee, Member of CIGRE Working Group JWG C1/C2/C6.18 (Coping with Limits for Very High Penetrations of Renewable Energy), International Technical Committee, and Member of CIGRE Working Group C6.30 (The Impact of Battery Energy Storage Systems on Distribution Networks), International Technical Committee.