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.