The major part of the electric grid modernization efforts includes utilizing a number of advanced computing, information, networking and measurement technologies. With these increasing cyber components, controlled synergy between heterogeneous physical power system and cyber components is required to meet the enhanced requirement of resiliency, security, and reliability. Security analysis requires analyzing vulnerability of the electric grid based on attack scenarios.

In this work, attack with incomplete information has been analyzed using graph theory based approach. Common attack vectors have been also utilized to operate breakers associated with generating resources to model aurora-like event. Real Time simulations for modified IEEE 14 bus test case system and graph theory analysis for IEEE 118 bus system will be discussed. This talk will also present real time modeling and simulation for cyber-physical system using smart grid test bed at Washington State University.