Abstract: Quantitative Methodology to Assess Cyber Threats in Electric Power System

Dong-Joo Kang[1], Sunju Park[1], Balho H. Kim[2], Koo-Hyung Chung[3]
Yonsei University[1], Hongik University[2], KERI[3]
dongjookang@gmail.com, boxenju@yonsei.ac.kr, bhkim@hongik.ac.kr, kchung@keri.re.kr

Abstract

This paper proposes a framework to assess cyber threats and vulnerabilities in control systems. The SCADA system is a representative control system and the power industry is using the largest one. The SCADA system used to be an isolated system on a local basis, but it is being connected into wide-area networks as the communication technology evolves. The Smart Grid is a full scale integration of energy systems and IT systems. The integration is bringing the existing cyber threats from IT systems. The power system requires a strong real time characteristic on the operation, which makes the cyber security context of the power system more complicated than general IT systems. For example, the availability is the most important aspect in control systems while the confidentiality is in information systems. In this context, it is required to assess the cyber security risks of the power system with a more systematic way. The risk is defined as the product of threats, vulnerabilities, and assets. This study proposes a framework for the assessment process for the risk components in the power system.

Acknowledgement

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education, Science and Technology (No. 2010-0022556)