2011 Japan-America Frontiers of Engineering Symposium
June 6-8, 2011
Tsukuba, Japan

Smart Grid Cyber Security

Mai Kiuchi
Central Research Institute of Electric Power Industry, Japan
mai@criepi.denken.or.jp

Abstract:

The smart grid has been described by IEEE as "a next-generation electrical power system that is typified by the increased use of communications and information technology in the generation, delivery and consumption of electrical energy". The smart grid is expected to have characteristics such as functions for self-healing from power disturbance, active participation by consumers in demand response, and other new products, services and markets. This means that there will be various devices connected to the communication network in the smart grid, and the network will not be closed within a certain utility, with bidirectional communications between the devices.

The above characteristics of the communication network for the smart grid leads to additional cyber security risks and problems in implementing security measures. An important point concerning the smart grid is that it is connected to a physical electric grid, so physical damage may occur from cyber attacks, which is different from cyber attacks in the Internet. In the past, control systems for the electric grid used proprietary technologies and standalone systems, which assured its cyber security to a certain extent. This would not be the case in the smart grid. As the communication network connects many devices, there are more potential intrusion points for the attacker. There may be difficulties in implementing security measures, as the control electric devices often have high requirements concerning latency and uptime. Applying security measures usually leads to additional latencies and system reboots, which would not be acceptable in a control system. Also, if home electronics such as air conditioners are connected, it would be difficult to ensure the cyber security of such devices. Furthermore, many of the devices may be physically easy to access, which means easier access to the system for the attacker.

We are considering methods to ensure the security of the communication system of the smart grid. First, we need to identify the assets in the system, the architecture of the components, and the data flow in the smart grid. Secondly, risk assessment has to be performed, including vulnerabilities, threats and impacts to the system. Third, the security requirements must be clarified for each of the components. Lastly, the appropriate security measures are selected.

Currently, the devices and network structure of the smart grid are unclear, which makes it difficult to identify the assets, architecture, and data flow in the system. We have considered the architecture to some extent with a rough system model, and selected security measures and their placement in the system.