CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

http: //d2.cigre.org
/

2017 Colloquium
September 20 to 22, 2017
Moscow – RUSSIA

Preferential Subject N°- PS2

The current security regulation of power control system in JAPAN and corresponding TEPCO PG's efforts

Teruki IWAMOTO, Mitsuyoshi KOYAMA, Tadashi OKABE
TEPCO Power Grid
JAPAN
okabe.t@tepco.co.jp

1 Security regulation in the power industry

In recent years, there has been an increase in awareness of the control system worldwide. In May 2016, industrial specifications by the name of “Guidelines for Power Control System Security” were created, and these are also applied to companies providing electrical services including gas companies and steel companies, etc. The ministerial ordinance was revised in September 2016 to adopt the guidelines into law, and thus a mechanism to legally regulate the security of the power industry was completed.

2 Overview of the power control system security guidelines

The newly established security guidelines comprise the following sections:

- Chapter 1 General provisions
- Chapter 2 Organization
- Chapter 3 Documentation
- Chapter 4 Security management
- Chapter 5 Security of Facilities and Systems
- Chapter 6 Security of Operation and Management
- Chapter 7 Security Incident Response

The requirements that are stipulated in the guidelines are set at either "Recommendation" or "Suggestion". "Recommendation" items are those that the operator should implement, and "Suggestion" items refer to items for which the decision to implement and the implementation method are left up to the operator.

These power control system security guidelines are characterized by its security management; specifically, the planning of appropriate security measures based on risk assessments (Plan),

implementation according to the plan (Do), inspection and report of the implementation results (Check), and considering readjustments (Action).

This risk-assessment-based approach greatly differs from the NERC CIP Standard which is classified as checklist type or prescriptive. The 32-page guidelines simply list the items for which security measures should be taken, and their objectives including problems in the event of insufficient measures. The guidelines stipulate “what” should be implemented, but do not stipulate “how” they should be implemented. This gives the electric utilities the flexibility to consider and introduce security measures that are most appropriate for the current status of their systems under their responsibility.

Variations of power control systems have been individually developed at Japanese utilities, and the equipment comprising these systems is geographically widespread and the installation environment is also diverse. Security measures can be efficiently taken against such systems in accordance with the risk assessment results.

3 Security efforts by TEPCO PG

The TEPCO group is focused on implementing thorough security measures of the power control system as host city of the 2020 Olympics. SIRT and SOC have already been launched at the TEPCO power grid, and full-scale preparations for the security framework of the OT (operational technology) system are underway.

The organizational size of TEPCO’s power grid is large, and each department has different systems. An umbrella organization is indispensable for responding to security accidents and also to implement the PDCA cycle for security measures. It was extremely effective to establish the SIRT and SOC framework for handling the legislation of the security guidelines.

Currently for SOC, network engineers are taking the lead in monitoring IDS and FW. However, we plan to monitor the power control system logs in the future as well. The networks of each system are isolated, but syslog protocol requires only unidirectional transmission, so we expect to be able to achieve uniform monitoring without increasing security risks. It is naturally ideal for SOC engineers to have advanced security skills. However, in the event of a security accident, the situation cannot be judged appropriately without being well-versed in operation of the power control system. Based on such reasons, we feel that it is necessary to develop SOC personnel in-house.

TEPCO PG shall continue to seek the ideal vision of power control system security while drawing upon IT (information technology) methods and the TEPCO group hopes to contribute to the enhancement of power control system security both in Japan and worldwide.