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°3

Evaluation of Cybersecurity Risks and Vulnerabilities of Advanced Metering Infrastructure Components

I. BENÍTEZ
Instituto Tecnológico de la Energía
Spain
ignacio.benitez@ite.es

V. GAVARA
Instituto Tecnológico de la Energía
Spain

A. QUIJANO
Instituto Tecnológico de la Energía
Spain

I. AGUADO
Instituto Tecnológico de la Energía
Spain

The present work is a study of the cybersecurity vulnerabilities and risks Advanced Metering Infrastructure (AMI) components may be exposed to, under the point of view that these components are seen as information technology devices and systems connected to a communication network. These components are first identified and described, evaluating the value of the information that they manage from the perspective of an attacker; then, the components vulnerabilities must be quantified.

The methodology applied identifies different criteria and defines scales, either quantitative or qualitative, to evaluate each of the AMI components according to each specific criterion, in order to globally evaluate each component's vulnerability and risks. The study follows the main cybersecurity guidelines and previous works in the area of Power Systems, such as the international standard IEC 62351 and the Smart Grid Architecture Model (SGAM) Framework defined by the European Work Group on Smart Grids Standardization. A special attention is also posed to the information management and the forthcoming Big Data technologies.

The summation of all these factors will determine the required efforts to protect each component from cyber attacks. These efforts, along with the type of attacker and the components' characteristics will allow to choose the countermeasures to be specifically addressed for each one. The level of physical protection of each field component is also studied.

The different criteria followed in this study are, among others, the scenario and Use Cases analysis; the types of threats that each component may face; the possible impacts of each of these threats and their quantification in a scale; and the selection of the countermeasures determined as most appropriate, from the possible actions described in IEC 62351 standard

and related communication standards such as IEC 61850 or Common Information Model (CIM).

The present study addresses the information management, from the field components of the AMI network (i.e. Meters and other monitoring equipment) through Data Concentrator devices, up to higher levels of information management. Two are the main physical communication network technologies addressed: Power Line (PLC) and Ethernet-based Wide Area Networks (WAN).