http: //d2.cigre.org
/

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

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

2017 Colloquium
September 20 to 22, 2017
Moscow – RUSSIA

Preferential Subject N°- PS2

Utility Information security at the dawn of IoT and NFV-enabled telecommunication service-chaining in cloud computing

Shuang Zhang
Stedin
The Netherlands
Blaak 8, 3011TA, Rotterdam
shuang,zhang@stedin.net

From an in-depth look at the fast-evolving landscape of the telecom sector, this paper begins with explaining why and how cloud computing and network function virtualization (NFV) are enticed the paramount role into the business with ever-strengthening industry traction. Equally the paper shares insight in how Internet of Things (IoT) technical specification at 3GPP (3rd Generation Partnership Project) proceeds to its completion, marking the advent of true IoT era with its agility to meet connectivity demands of various industries, known as “vertical industries” of IoT.

From electrical utility’s perspective, such advancements seem to be only the next-door excitement. However, the truth is that the electric utility sector is well impinged on with these new technological development. For instance, the perpetual quest for high availability and reliability for transmission of quality power is safeguarded with mechanisms of EMS, DMS, tele-protections, load-balancing, MLI voltage stability control, etc. These means, both in their current and future form all depend on carrier-grade telecommunication infrastructure. In the meantime, remote control and real-time interaction with a large number of medium voltage substations not only inspires smart-grid application versatility, but also places challenge on communication infrastructure.

Hence this paper focuses on discerning the application boundaries of these advances in information and telecommunication systems, from the electrical utility information security point of view. Further breakdown of this paper would be:

1. IoT and architectural impact on information security;
2. Cloud NFV architectural impact on information security;

In order to put the analysis into perspective, this paper will include a case study, where Cloud NFV and IoT are used to deploy a tailor-made Network as a Service (NaaS) for two business services, namely Tele-protection, and MV/LV substation control and management using IoT. The related concerns of information security are reasoned accordingly.

To conclude, this paper recommends applicability of and remedies for these technologies regarding information security practices in the electrical utility.