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

BUILDING A SECURE NETWORK FOR NEW SCENARIO CASE: CHESF

RODRIGO LEAL (*)
CHESF
BRAZIL

UBIRATAN CARMO
CHESF
BRAZIL

(*) rodrigol@chesf.gov.br

The technological convergence, especially with the implementation of IP protocols, it points to increasing network integration of various segments of the electricity sector companies, including its administrative and operational areas, which brings large increases in process efficiency of these companies, but while requiring greater investment and concerns about information security.

In recent years, the global energy industry was hit by cyber attacks more than any other industry in the world. Energy installations - including operations in the electricity sector and oil and gas - are increasingly vulnerable to cyber attacks that can lead to service interruptions or loss of information. Costly disaster, with the potential to cause further environmental damage, lack of power supply for weeks or months, and even loss of human life. In addition to the increased frequency of incidents, attacks on energy companies are becoming more sophisticated, making them more difficult to detect, fight and defend themselves.

Despite the "cyber war" be in greater evidence in the international sector and greater focus on first world countries, Brazil - as an emerging and the growth of the energy sector country - has already suffered the consequences. Brazilian companies are far from immune and are great targets for such attacks. Brazilian companies are starting only now to invest in cyber security, while, for example, the US have done a decade ago. Operators of critical infrastructure and energy utilities need to become aware and be prepared - as the trend is only increasing.

A successful cyber attack on SCADA systems has the potential to seriously disrupt critical business operations. Problems with software, human factors of IT and new vulnerabilities brought by the trends of digital operations have a multiple set of risks exposed to vulnerabilities.

Currently, much of the cyber security of CHESF is based in the domain access control which protects against external threats, within this domain the protection is carried out at the

application level. The domain access control service is managed by IT and the applications level is managed by the application's owner. However, with the convergence technology, with integrated network and with the current landscape area of Telecommunications and Automation has been working to implement operational security solutions, ensuring greater reliability the Electric System.

The projected layer of security aims to provide protection to all features of the CHESF telecommunications system, existing and new specified in the Telecommunications Director Plan – Horizon 2023 that make use of its infrastructure, and should provide strength and capacity to support the migration of many corporate and operational services that are supported by the Telecommunications network, such as telephony, dispatch, SCADA, Disturbance, Qualimetry, video conferencing, video surveillance, among others, for the IP platform.

The security layer is composed of hardware and software resources to ensure the protection of information and CHESF network devices. The design and implementation of specified security layer shall be in accordance with the recommendations of standard-setting bodies. The security layer of CHESF requirements ensure the date within your organization stays within your organization, ensure your mission-critical network is 'always on' and under full control and protect the privacy of your employees and customers.

Thus, it is increasingly necessary to interactively discuss the main challenges for cyber security measures in the industry to ensure the safety of information, communications and critical infrastructure assets of the Brazilian energy sector.

This article is structured as follows: The first section presents the context of telecommunications infrastructure on the current model information and the interface of this model with the flow of operational information and not operational information addressing the particular characteristics of the company. The second section will deal with the physical and logic architecture o cyber security address to Telecommunication Network as the main means of transporting information and how to ensure the transport safety. The third section addresses the security architecture and the interfaces of the transport routes and applications domains of automation technology (AT) and information technology (IT) and finally the conclusions.