CONSEIL INTERNATIONAL DES GRANDS RÉSEAUX ÉLECTRIQUES
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°- PS3

Challenges to Implement Secure Remote Services

V. TAN
PSC Consulting
Australia
victor.tan@pscconsulting.com

D. HOLSTEIN
OPUS Consulting Group
United States
holsteindk@ocg2u.com

M. SEEWALD
CISCO
Germany
maseewal@cisco.com

Remote services to access EPU communication networks continues to create significant security challenges to address the evolving threats. EPUs must meet these challenges by adjusting organizational responsibilities, improving personnel training to recognize unauthorized access and use of their networks, and keep pace with new local laws and regulations, and take advantage of technological advances that can improve remote access security.

CIGRE SC D2 has commissioned a new working group, D2.40 to address the evolving threat landscape. This working group created several work streams to focus attention on specific topics. The topic for work stream 3 is to examine the new technologies and connectivity to assess the risks and potential means to mitigate these risks. An early task, which is the subject of this paper, is to develop a coherent model of the applicable remote service requirement objectives.

IT security in remote services is a complex subject that requires equal attention be given to local laws and regulations, operating and organizational constraints imposed by the EPU, and technical and non-technical controls to securely operate and manage remote services. Navigating the complexity of security requirements from applicable standards and guidelines is the challenge addressed in this paper. This paper describes two of the tasks performed to meet this challenge:

1. Discuss network security design (segmentation, threat detection, and mitigation – a reference architecture. For example, IDS and IPS to trigger alarms, and to recommend that alarms be output to a specified interface (62351-7), such as to an integrated security operation centre (ISOC). Also note that alarm data can be processed to generate valuable access control statistics.
2. Identify and characterize the fundamental security requirement objectives imposed on implementation and operation of EPU remote services. Also, address the relationships between fundamental security requirement objectives and their relationship to the local operating environment.