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°- 2

About cyber physical model for cybersecurity researches in power industry.

ALEKSANDR VOLOSHIN, OLEG ARKHANGELSKIY, FEDOR IVANOV
MPEI, RTEC, EnLAB
Russia
mail@ennlab.ru

The widespread introduction of information technologies and computing technics at power facilities acutely raises the issue of their resilience to vulnerability to cyber threats. Degree assessment of the impact of cyber threats in the power industry can not give full understanding of the real impact of cyber attacks only by analysis of control and networks communications systems (CNCS).

It is necessary for a complete assessment of the estimate of loss to analyze different power system failures which have been induced by cyber attacks to CNCS. This requires the use of specialized cyber physical simulators (CPS) of power systems. They simultaneously work like the power system model and like CNCS model. The using of such CPS allows to assess the vulnerability of equipment impact to cyber attacks considering increase of the infected equipment trip time, loss of the power system stability, etc.

For these targets RTEC company creates a large CPS. It is based on the RTDS simulator which creates a virtual model of power system primary equipment including substation 220/110/6 kV. For realizing of secondary equipment in CPS is used as real devises and systems as and their virtual models made by RTDS. Designed CPS allows to assay different information protection facilities and conduct their certification tests. There are considered the main technical solutions used during CPS designe, specified the application features of CPS for cybersecurity researches in the report.