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

Possible approaches to cybersecurity threat modeling in the Power Grid

V. KARANTAEV
INFOTECS
Russia
Vladimir.karantaev@infotecs.ru

Threat model development is a typical well-recommended method of analysis that is used by cyber security experts. The result of their work is making an assumption about immediate and non-immediate (potential) cyber security threat existence. The result is described in terms clear to industry experts. Real experience of using traditional methods usually used in bank and state sectors failed because the assumption about the possibility of corruption of information characteristics (properties) such as availability, integrity, confidentiality, authenticity and non-repudiation do not allow to conclude that cyber attacks can have a direct influence on the technological process continuity, which is the main purpose of providing information security of automated control systems. Reaching the goal of a precise assumption about the influence of immediate threats, found in automated control systems, on the electrical power network technological process continuity is flawed by several factors:

- Existing terminology database used by different industry experts;
- Choice of security object (transforming substation, grid control centre, automated control systems or the whole power system in general);
- Existing methodology of threat modeling;
- Choice of an approach to categorizing computer incident results.

The possible approach to threat modeling in automated control systems might be an approach based on making an assumption about possible effects on a power system object, a power system sector and a power system in general. This approach will allow to conduct documents applicable to practical usage by a wide range of experts such as information security experts, protection

engineers, SCADA engineers, operators, engineering services, i.e. main participants of the process of making reliable and safe electrical grid facilities.
The most valuable are documents supporting subjective conclusions made during threat modeling because the precision of threat models much depend on the qualification of experts who modeled these threats. Objective results of experiments done to prove or argue against the obtained result can be conducted during the development of a cyber physical testing facility modeling power system sector operation.
Based on the results of two complementing each other methods it is possible to conclude not only about the necessity of applying this or that security method, but also about the applicability of the security methods that can be recommended after completing the first stage of work.
Methods of threat modeling based on different methodological approaches, such as forensic studies, mathematic modeling and experiment conducting, come forward for discussion.