1. RATIONALE

Nowadays Large Complex Critical Infrastructures (LCCI) are operated and monitored thorough complex IT Systems and electric systems are not an exception.

Extraordinary natural phenomena or human made malicious attacks can be directed against the physical elements of the system or to the IT systems that control system operations.

IT systems allow the operators to receive real time information from the field and rely on a number of processes and applications that assist them to take decisions.

IT systems permit the operator to execute the decisions taken in order to change the generation and voltage profiles or introduce changes in the system topology which will modify the system flows. In exceptional occasions can also reduce the system demand.

Malicious attacks may target IT systems to disturb the control of the system or to impact to the physical system in order to produce local, regional or national blackouts.

The IT systems under possible threats are:

a. The computer systems placed in Control Rooms at control National, Regional and Local Systems to limit the operators automatic or manual control capacity.
b. The power plants control rooms that may modify the generation profile or even impact in the security of some of the power plant elements.
c. Substations, that in most cases are unattended, the IT local and remote supervisory control and data acquisitions (SCADA's) or the Intelligent Electronic Devices (IED) placed in substations with the mission to control and protect their active elements.
d. The intensive use of communications, public and private, to link all those elements are at the same time possible targets for malicious activity.

The Control IT Systems are sensitive to extraordinary meteorological incidents that may impact on their availability or performance, but are also attractive for malicious attacks due to the impunity for the attacker who acts away from the Control Centres in case of hijack.

The impact of these threats is twofold:

a. Reduce the control capacity of system operators by limiting their information, with consequences in the decision making processes, or reducing its capacity to implement those decisions. This situation will carry an immediate loss of control over the system which in the medium term, if not corrected, may impact on the electric energy users.
b. The malicious use of the IT systems may directly impact on the physical layer and modify topology, generation or any other system parameter. This may influence into the system performance and