About the key role of cyber security in power system resilience

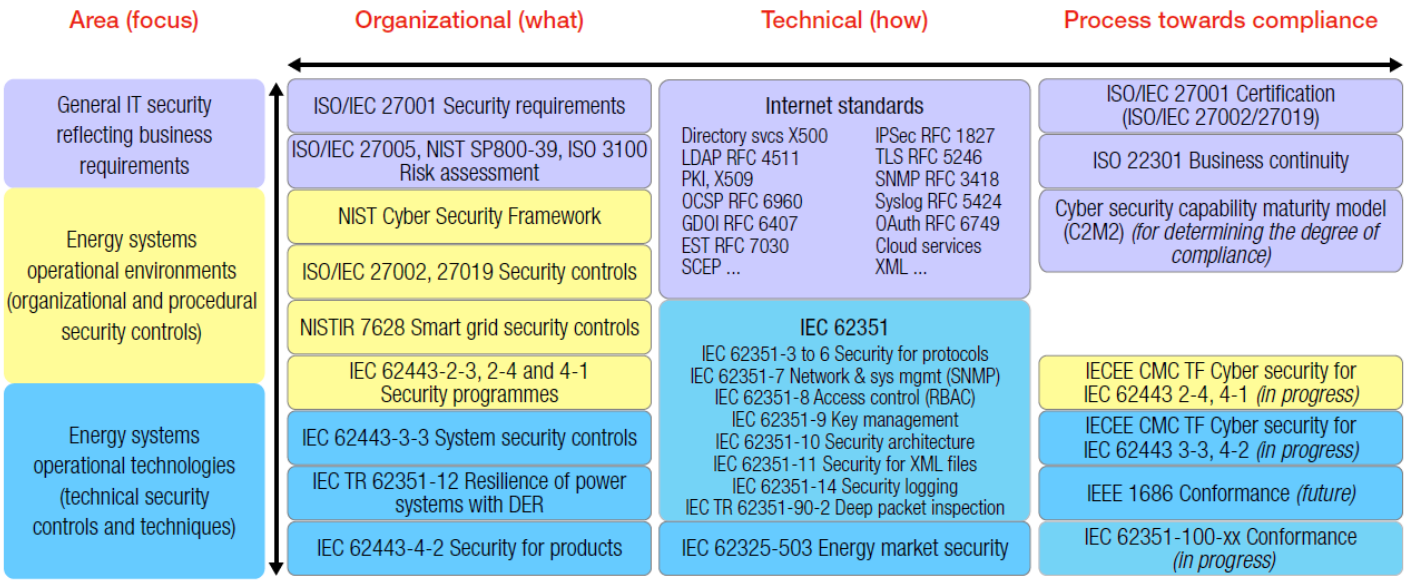
Olga Sinenko, SC D2 Chair
Olga.Sinenko@cigre.org

Giovanna Dondossola,
AG D2.02 (Cybersecurity) Convenor
Giovanna.Dondossola@rse-web.it

With the progressive digitalisation of electric power processes imposed by the ongoing energy transition, power operators need to implement an effective cyber security strategy within their organisation. As providers of the most essential service to the society and the economy, such cyber security strategy is aimed at managing the risks from cyber threats to the information and communication infrastructure and making the power service operation resilient to cyber incidents. This paper presents a harmonised view of the role of cyber security for the power system resilience, extracted from the CIGRE activities performed by the Advisory Group D2.02 and the Working Group D2.46. By making reference to the key standards for the implementation of cyber security strategy, it provides a summary of the most effective best practices and a view of future developments and planned CIGRE activities.

The definition of the term “resilience” depends of the field of interest. Focusing on power systems, it could be considered that a resilient infrastructure is that one capable to be recovered after the occurrence of an adverse situation. CIGRE Working Group C4.47 introduced a definition of power system resilience as “the ability to limit the extent, severity, and duration of system degradation following an extreme event” that is achieved through measures to be taken before, during and after extreme events.
When extended to cyber-power systems, the definition requires to focus on the attack process dynamics and evolution in order to adopt security protections to the digital infrastructures to be taken before the occurrence of cyber threats, as well as security measures that apply during ongoing attacks and after that a targeted attack succeeded in provoking a serious cyber incident to the utility business continuity, with possible impact on grid users. Lessons learned from real attack cases reveal that there is a great space for improvement in an organisation’s defence capability by introducing anomaly detection measures along the attack timeline.

The strong connection between cyber security and power system resilience is confirmed by the North American Electric Reliability Corporation (NERC) when they state that resilience is a component of reliability in relation to an event, and once cyber security is a key issue to reliability as can be found in the NERC CIP regulation CIP-008-5 stating requirements for “Cyber Security - Incident Reporting and Response Planning”, for example.
As of today, most national level cyber security strategies use the NIST Cybersecurity Framework as a reference for defining cyber resilience strategies of cyber-physical systems. The framework distinguishes the requirements for identify, protect, detect, respond and recover from cyber threats within a critical infrastructure organisation.
For guiding the energy operators in the implementation of their cyber resilience strategy the Cyber Security Task Force of the IEC System Committee Smart Energy has selected a set of international standards that apply to smart energy operational environments.



(Click on the figure to enlarge it)
Figure 1 - Key cyber security standards and guidelines

[Source: IEC Technology Report: Cyber security and resilience guidelines for the smart energy operational environment]

As can be seen from the series of standards in Figure 1, organisational security controls have to be combined with technical controls to be implemented at both system and product level by system integrators and device producers. The implementation of technical controls (third column in Figure 1) is based on standards developed by the Internet related organisations and by committees from the energy sector. This gives evidence to the convergence of IT and OT technologies and the need to make them interoperable, an issue that is even more relevant with the deployment of open platforms based on IoT technologies, and edge and cloud-based services.

According to the best practices recommended by standards and guidelines, the security requirements of authentication, authorisation, integrity and accountability rely primarily on cryptography and require electronic key and certificate management systems, while availability requirements are mainly addressed by means of network segregation techniques and system engineering practices for configuration and redundancy management.

As a future contribution to the cyber-power system resilience, it is worth mentioning the recently launched CIGRE WG D2.50 on the management of cyber security for contingency operations, including the identification of cyber security over-ride requirements to gain access to and use of protection, automation, and control system assets that should be included in policies, procedures, and organizational directives related to emergency procedures and restoration operations. A further topic addressed by undergoing research activities concerns the calculation of combined metrics linking cyber security indicators with resilience indexes for assessing, for example, at what extent delayed or missing information due to successful attacks affects the ability to utilize the available resources for system recovery.

Another just started CIGRE WG D2.51 focusses on studying and analysing the current maturity level of theory and practice in the Security Operation Centers within the electric power industry. The main aim of this group is to provide an overview of worldwide experience in the Security Operations Centers and cyber situational awareness spheres and develop practical recommendations for their development to be used by a wide range of specialists. A technological advancement of security information and event management is represented by the development of anomaly detection platforms based on machine learning techniques.
For more details on the activities related to cyber-power resilience presented in the paper, the interested reader is invited to read the technical papers and/or brochures published by the WGs on the CIGRE electronic library e-cigre.