CIGRE Study Committee D2

PROPOSAL FOR THE CREATION OF A NEW WORKING GROUP

WG [1]N° D2.51	**Name of Convenor:** Vladimir Karantaev (RU) **E-mail address**: Vladimir.Karantaev@gmail.com
Technical Issues #[2]: 2	**Strategic Directions #[3]: 1,2**
The WG applies to distribution networks[4]: Yes	
Potential Benefit of WG work #[5]: 3	
Title of the Group: Implementation of Security Operations Centers (SOC) in Electric Power Industry as Part of Situational Awareness System	

Scope, deliverables and proposed time schedule of the WG:

Background:

Today digitalization is one of the key factors of Electric Power Industry developing strategy. The electric power industry is changing. These changes could influence the structure of power energy systems and principles of process operation. The electric power industry has some practical experience in realization of IEC 61850 requirements, engineering and implementation of digital substations.

Positive and negative effects have been found out. For example, Information and communications technologies (ICT) used in digital substations are vulnerable to cyber-attacks. The most of ICTs are insecure by design. Since technology stack of Industrial Internet of Things and Smart Grids could be developed and used extensively, successful Advanced Persistent Threats (APT) attacks could be serious risks. These risks could result in cyber and physical damage to digital substation and Smart Grids characteristics.

In order to minimize risks of successful cyber-attacks it is necessary to improve approach to cybersecurity of future automation systems of Power Energy.

Experts of the electric power industry should consider the possibility of creating a secure by design digital substation. The cybersecurity subsystem should become a part of digital substation as a typical technological subsystem with cybersecurity technologies up to the set of requirements of process automation systems.

It is important to manage cybersecurity at each level of engineering and development of Energy Facilities. According to national requirements, Power Utilities in many countries must organise, build or use Security Operations Center (SOC) for protecting their infrastructure including OT segment. Extensive usage of SOC as a part of Situational Awareness system could help to improve the management of cybersecurity. Moreover, Situational Awareness system itself might be changing. Using of Security Operations Center (SOC) could improve Situational Awareness about cyber threats and avoid confusion with situational awareness in control centres about power flows.

Earlier in CIGRE documents WG B5.66, "Cybersecurity requirements for PACS and the resilience of PAC architectures" and WG D2.46 "Cybersecurity: Future threats and impact on electric power utility organizations and operations" Annex D Integrated Security Operations Centre the theme of SOCs, ISOC was raised. For example, the Technical Brochure WG D2.46 includes the main information about ISOC structure, security events sources, description of usage benefits. The new group will continue this work and propose more comprehensive point of view.

Scope:

1. The first part of group work will involve a **survey of use of SOC in utilities worldwide,** reviewing, exploration and analysis of national regulations in cybersecurity sphere in relation to mandatory implementation of SOC for EPU.
2. A second part of group work will involve reviewing, exploration and analysis of dedicated IEC/ISO/IEEE standards in field of cybersecurity of Power Grids (Smart Grids). Preparing recommendation for development if it is needed.
3. Learning and analysis of cybersecurity best practices for building and organising internal or outscoring IT and OT SOCs.
4. Development of recommendations for building and organising integrated SOC in EPU.
5. Development **of requirements and architectures of the new SOCs** in EPU.

The WG will make reference to the work of the following WGs as applicable:

- WG B5.66 "Cybersecurity requirements for PACS and the resilience of PAC architectures".
- WG D2.46 "Cybersecurity: Future threats and impact on electric power utility organizations and operations".
- WG D2.38 and it`s TB 698 «Framework for EPU operators to manage the response to a cyber-initiated threat to their critical infrastructure» was published in September 2017.

Deliverables:

☒ Technical Brochure and Executive Summary in Electra

☒ Electra Report

☒ Tutorial[6]

☒ Webinar[6]

Time Schedule: start: October 2019 **Final Report**: September 2022

Approval by Technical Council Chairman:

Date: November 19th, 2019

Notes: [1] Working Group (WG) or Joint WG (JWG), [2] See attached Table 1, [3]See attached Table 2, [4] Delete as appropriate, [5] See attached Table 3,
[6] Presentation of the work done by the WG

Table 1: Technical Issues for creation of a new WG

1	Active Distribution Networks resulting in bidirectional power and data flows within distribution levels up to higher voltage networks
2	Digitalization of the Electric Power Units (EPU): Real-time data acquisition includes advanced metering, processing large data sets (Big Data), emerging technologies such as Internet of Things (IoT), 3D, virtual and augmented reality, secure and efficient telecommunication network
3	The growth of direct current (DC) and power electronics (PE) at all voltage levels and its impact on power quality, system control, system operation, system security, and standardisation
4	The need for the development and significant installation of energy storage systems, and electric transportation, considering the impact they can have on the power system development, operation and performance
5	New concepts for system operation, control and planning to take account of active customer interactions, and different generation types, and new technology solutions for active and reactive power flow control
6	New concepts for protection to respond to the developing grid and different generation characteristics
7	New concepts in all aspects of power systems to take into account increasing environmental constraints and to address relevant sustainable development goals.
8	New tools for system technical performance assessment, because of new Customer, Generator and Network characteristics
9	Increase of right of way capacity through the use of overhead, underground and submarine infrastructure, and its consequence on the technical performance and reliability of the network
10	An increasing need for keeping Stakeholders and Regulators aware of the technical and commercial consequences and keeping them engaged during the development of their future network

Table 2: Strategic directions of the Technical Council

1	The electrical power system of the future: respond to speed of changes in the industry
2	Making the best use of the existing systems
3	Focus on the environment and sustainability
4	Preparation of material readable for non-technical audience

Table 3: Potential benefit of work

1	Commercial, business, social and economic benefits for industry or the community can be identified as a direct result of this work
2	Existing or future high interest in the work from a wide range of stakeholders
3	Work is likely to contribute to new or revised industry standards or with other long term interest for the Electric Power Industry
4	State-of-the-art or innovative solutions or new technical directions
5	Guide or survey related to existing techniques; or an update on past work or previous Technical Brochures
6	Work likely to contribute to improved safety.
7	Work addressing environmental requirements and sustainable development goals.