CIGRE Study Committee D2

PROPOSAL FOR THE CREATION OF A NEW WORKING GROUP

WG [1]N° D2.50	**Name of Convenor:** Dennis Holstein (US) **E-mail address**: holsteindk@ocg2u.com
Technical Issues #[2]: 1, 2	**Strategic Directions #[3]: 1, 2**

The WG applies to distribution networks[4]: Yes

Potential Benefit of WG work #[5]: 3, 5, 6

Title of the Group: Electric power utilities' cybersecurity for contingency operations

Scope, deliverables and proposed time schedule of the WG:

Background:

Multiple standards and CIGRE technical brochures have discussed the requirements for cybersecurity defense-in-depth and its impact on protection, automation and control systems (PACS) operations. However, IEC 62443 and IEC/TR 63069 include technical controls to ensure that security does not interfere with safety requirements. In addition to safety, emergency and contingency situations require over-ride of cybersecurity controls imposed on PACS assets. Executing the over-ride of cybersecurity controls must be performed under positive control to minimize interruption of operations and be completed in a timely manner to return the system to a secured state. Implementing over-ride and recovery must be seamlessly integrated into the electric power utility's (EPU's) crisis management policies, procedures, and organizational directives.

Effective management requires some metrics such as:

- Time from program launch to deployment of simplest functionality.
- Time to field high-priority functions.
- Time required for full regression test (automated) and cybersecurity audit/penetration testing.
- Time required to restore service after an interruption or outage.
- Number of bugs caught in qualification testing versus deployed testing.

As noted in the research, the means to implement the tenants of a strategic cybersecurity policy requires attention to three topics – in short, people process, and technology:

1. Technical controls of security are the mechanisms that protect EPU systems from incidents or attacks: Antivirus software, access controls, backups, recovery and audit software, for example.
2. Formal controls of security are EPU's business structures, processes and metrics that ensure the correct general conduct of business and reduce the probability of an incident or an attack, or at least measure and minimize its impact. For example, separating the security organization from other IT and OT departments, designing correct segregation of security duties and therefore access rights and privileges, designing and controlling the appropriate employee-supervisor relationship, routine risk evaluations, etc.
3. Informal controls essentially deal with the culture, value and belief system of the EPU. An organizational culture in which it is possible to understand management' s intentions, and which is conducive to developing a shared vision and other informal objectives, would make members of IT and OT more committed to their activities and success. Informal controls might be created, for example, by increasing awareness of security issues through education and training programs.

For the most part, CIGRE technical brochures, applicable standards, and open source documents are silent on what metrics to gauge, and what over-rides are needed and how they would be managed and enabled completed in a timely manner. The challenge is to devise a management schema that is highly adaptable to the dynamics and complexity of known and unknown threats. The research of CIGRE TB 698, Annex C, and the current work in CIGRE D2.46 and B5.66 introduced the use of model-based system engineering (MBSE) describe the logical architecture of the system of interest (SoI). MBSE is well suited to address the issues of contingency operations of the selected SoI.

Scope:

Investigate the following subjects:

1. Identify the situations that require consideration of cybersecurity over-rides to gain access to and use of PACS assets.
2. Provide supporting analysis and use cases for enabling over-ride mechanisms to ensure access to and use of PACS assets.
3. Identify cybersecurity over-ride requirements that should be included in policies, procedures, and organizational directives related to PACS operation.
    a. Describe the processes and interaction of organizational units to ensure cybersecurity over-ride requirements are implemented in accordance with local laws and regulations.
    b. Identify the skills and training required to effectively manage over-ride operations.
    c. Describe the processes needed to reactivate security controls to return to normal secure PACS operations.
4. Develop classes of metrics that can be used by other CIGRE study committees to quantify cyber-physical security solutions in terms of deployment rate, response rate, and degree of complexity. An approach like the US Defense Innovation Board metrics for software development should be considered, among others

Deliverables:

☒ Technical Brochure and Executive Summary in Electra

☒ Electra Report

☒ Tutorial[6]

☐ Webinar[6]

Time Schedule: start: January 2020 **Final Report**: December 2023

Approval by Technical Council Chairman: Marcio Szechtman

Date: November 18,2019

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.