CIGRE Study Committee B5 – Protection - Automation

PROPOSAL FOR THE CREATION OF A NEW WORKING GROUP (JWG)

JWG* N° B5/D2.46	**Name of Convenor:** Dennis K. Holstein (USA) **E-mail address**: holsteindk@ieee.org
Technical Issues # (2): 6	**Strategic Directions # (3):** 1
The WG applies to distribution networks (4): Yes	
Title of the Group: Application and management of cyber security measures for Protection & Control systems	

Scope, deliverables and proposed time schedule of the Group:

Background:

Cyber-security threats, whether real or imaginary, are becoming more and more publicized. Attacks such as the Stuxnet worm have revealed that Industrial Control systems are more insecure than was believed. But there seems to be no end of guidelines, standards and best practices that all claim to provide some defense against the threats and attacks.

Standards such as NERC CIP, IEEE P1686, ISO/IEC 2700X, IEC 62351 and IEC 62443 propose various mechanisms for providing cyber-security into substations and on protection relay equipment. These standards, though, have different approaches and objectives. For example, IEC 62351 scope includes protocol requirements to ensure security interoperability, while IEC 62443 scope includes the allocation of system requirements to subsystems and components. Some standards define measures that include encryption requirements for authentication, integrity, and privacy. Sophisticated schemes for remote and local role based access control (RBAC) are also proposed. These security schemes are based on the deployment of advanced technologies for substation automation and protection relays.

Faced with the ever-increasing threats but overwhelmed with the plethora of standards and guidelines, what practical organizational and technical guidelines for implementing cyber security in a digital substation protection and control (P&C) system need to be developed? What actually are these threats and what action(s) would be required by the protection and control engineer if such a threat occurs?

This JWG will build on the output from B5.38 (The Impact of Implementing Security Requirements using IEC 61850) and D2.22 (Information Security for Electric Power Utilities) and the on-going D2.31 (Security architecture principles for digital systems in Electric Power Utilities (EPUs)), but will focus on considering the available standards and determining how they can be effectively deployed and managed by Protection &Control engineers for Digital Substation Automation System (DSAS) and protection relays, and whether the security breaches on protection and control applications are mitigated by their respective recommendations.

In close cooperation with CIGRE SC D2, this JWG will extend D2's security framework recommendations to include Protection & Control operating constraints. Close cooperation will be enabled by common membership in the JWG and CIGRE WG D2.31. The objective is to avoid duplication of work related to management of remote third-party access, role-based access control, and other topics which have been examined extensively by D2 and others.

Scope:

1. Perform a study to identify the threats to the protection and control system and analyze the proposals in the standards to evaluate their effectiveness in providing a defense against the identified P&C threats. Identify real risks to critical P&C system components. For example, outside access via SCADA controls known as the man-in-the-middle scenario.

2. Analyze the standards to identify differences and propose practical organizational and technical guidelines for implementing cyber security in a P&C system that minimizes these differences. This analysis also covers the evaluation of performance deterioration of IP based systems, as IEC 61850 based Digital Substation Automation System (DSAS), due to the implementation of cyber security features.

3. Based on IEC 62351 and other relevant standards, recommend mitigation strategies to be implemented in substation Protection and Control. A particular focus will be given on:

- based on existing standards and guidelines, application of RBAC to Digital Substation Automation System (DSAS) and protection relays.
  - What roles are appropriate?
  - Address how operations such as settings download or disturbance record extraction could be categorized
  - What could be proposed as standard roles and associated rights?
- based on existing standards and guidelines, application of encryption to DSAS and protection relays
  - Certificate management: consider what schemes are appropriate for P&C systems, e.g. configuration of an IED's certificates
  - Performance constraints: impact of encryption overhead on protection relays versus compensating security schemes.
- based on existing standards and guidelines, application of authentication to DSAS and protection relays
  - User identities and passwords: Limitations of data entry via front panels.
  - Centralized versus distributed authentication of user credentials.
  - Visibility of alarm state or rapid access to controls that require access and use authentication.
  - Management of complex passwords: simplification is needed for field operations and real time control.
- Issues related to the cyber security of Digital Substation Automation System (DSAS) and protection relays (in co-operation with D2.31)
  - Contractual relation and organization with third-parties having remote access to DSAS, e.g. DSAS and relay manufacturers,
  - Organizational measures for DSAS and relay operation staff.
  - Organizational measures for DSAS and relay maintenance staff.
- Recommended requirements concerning cyber security in specifications for Digital Substation Automation System (DSAS) and protection relays .

4. Describe real world examples of 'normal' DSAS and protection relay operation to evaluate the security impacts arising from these. Consider security issues that arise from such protection and control operations as follow:

- Technician uses a USB memory stick into the substation HMI of the DSAS or the protection relays (sitting inside the firewall) in order to upgrade some Protection & Control software.

- Technician connects a multipurpose laptop (possibly even 3G enabled) to the DSAS substation bus or to protection relays.
- Technician connects a special test set to the DSAS substation bus or to protection relays.

Deliverables: Technical brochure with summary in Electra, and a summary PowerPoint presentation.

Time Schedule: start: 2012 **Final report**: 2014

Comments from Chairmen of SCs concerned:

Approval by Technical Committee Chairman: Klaus Fröhlich

Date: 01/03/2012

(1) Joint Working Group (JWG) – (2) See attached table 1 – (3) See attached table 2
(4) Delete as appropriate

Table 1: Technical Issues of the TC project "Network of the Future" (cf. Electra 256 June 2011)

1	Active Distribution Networks resulting in bidirectional flows within distribution level and to the upstream network.
2	The application of advanced metering and resulting massive need for exchange of information.
3	The growth in the application of HVDC and power electronics at all voltage levels and its impact on power quality, system control, and system security, and standardisation.
4	The need for the development and massive installation of energy storage systems, and the impact this can have on the power system development and operation.
5	New concepts for system operation and control to take account of active customer interactions and different generation types.
6	New concepts for protection to respond to the developing grid and different characteristics of generation.
7	New concepts in planning to take into account increasing environmental constraints, and new technology solutions for active and reactive power flow control.
8	New tools for system technical performance assessment, because of new Customer, Generator and Network characteristics.
9	Increase of right of way capacity and use of overhead, underground and subsea infrastructure, and its consequence on the technical performance and reliability of the network.
10	An increasing need for keeping Stakeholders aware of the technical and commercial consequences and keeping them engaged during the development of the network of the future.

Table 2: Strategic directions of the TC (cf. Electra 249 April 2010)

1	The electrical power system of the future
2	Making the best use of the existing system
3	Focus on the environment and sustainability
4	Interactive communication with the public and with political decision maker