IEEE Power System Communication & Cybersecurity Committee

CYBERSECURITY SUBCOMMITTEE – S0

IEEE JTCM - Jacksonville, FL

Chair: Steven Kunsman

Vice chair, Jim Bougie

Secretary: Farel Becker

S0 website: http://sites.ieee.org/pes-pscc/cybersecurity-subcommittee-s0/

Minutes – January 10, 2018

1. **Introductions** 18 attending by the end of the meeting
2. **Quorum:** 10 of 14 members in attendance and a quorum was reached
3. **Approval of the minutes from the last meeting:**
    a. September 2017- Minutes were not approved due to lack of a quorum at the beginning of the meeting. Steve took the action to send out the minutes to S0 members.
    b. There was a discussion about how to become a Subcommittee member and the importance of signing the sheet.
        i. Requirements for SC membership
            1. Be a member of IEEE PES
            2. Be an active member of S SC working group(s)
            3. Be willing to regularly attend and participate in the S SC
4. Working Group Report
    a. WG S1: 1686
        i. Marc Lacroix reported that their group met and started the process of setting up the report structure for moving forward.
            1. Next meeting will be in May in Pittsburgh
    b. WG S2: P1711.1 Serial SCADA Protection Protocol (SSPP)
        i. This group did not meet and looking for a new chair due to the resignation of Dave Whitehead
        ii. This working group received a one year par extension

iii. Steve took an action to talk to Craig and Mike about finding a replacement Chair and Vice Chair

c. WG S3: P2030.102.1 Standard for Interoperability of IPSEC Utilized within Utility Control Systems
   i. James Formea provided an update. A remaining set of comments needs to be resolved. The working group is looking for some IPSEC experts to help finalize the standard.
   ii. PAR was extended to December of 2019

d. WG S4: P1711.2 Trial-Use Standard for Secure SCADA Communications Protocol (SSCP)
   i. Steve explained that this working group did not meet in Jacksonville. Draft standard is being finalized to proceed for MEC review.
   ii. WG PAR had previously extended to Dec 2018

e. WG S5: Cyber Security Requirements for Power System Automation, Protection and Control Systems
   i. WG PAR was approved allowing the group to meet.
   ii. Steve explained that during the meeting the identified gaps were discussed and assignments made to begin drafting work.
   iii. TW Cease has volunteered to be WG Vice-chair.

f. TF S6: IoT for connected home - Communication and cybersecurity requirements
   i. Marc reported that the task force has started work on producing the report.
   ii. A major focus of the task force will be to prepare the requirements for IOT outline use cases for the report such as demand response connect by the utility
   iii. James Formea has been appointed as vice-chair.

g. TF S7: Electrical Power System Cyber Device Function Numbers, Acronyms, and Designations
   i. Nathan discussed how they plan to develop logical node name for Cyber Security functions such as a firewall.
   ii. Herb Falk stated that it might be better to develop this as a Brick rather than a logical node.

h. TF S8: Testing Power System Cybersecurity Controls

i. Nathan presented a PAR at the First meeting to be voted on by the sub-committee. The PAR was reviewed, brought to a vote and was approved by the SC. The PAR request will be submitted to the main committee on 1/11/2018 for vote and approval.
ii. Nathan's vision for this report is to eventually develop an IEEE Guide for Cybersecurity Testing in Electric Power Systems

5. Old Business
    a. There was an IEEE Cyber Security Workshop held adjacent to the December NERC CIPC meeting in Atlanta (Steve, Nathan and Mike Dood participated).
        i. A whitepaper is in process. About 60 people attended with 17 presenters.
        ii. There was a positive response as well as input was to have the meeting in parallel in June.
    1. Open action remains: In S4, Rich Corrigan discussed SSP21 as an open source code led by California Energy Systems for the 21st Century (CES21). The group agreed to review this topic and make a presentation next meeting and it would fall under the new work of the 1711 general document activity. This did not take place at the January meeting. Since this did not happen of this in the January meeting, Scott Mix and Mark Hadley have an action to coordinate the demonstration to compare these two protocols. Herb Falk raised the concern if the demonstration is for the purpose of comparison, a set of metrics needs to be defined.
6. New Business
    a. Joe Weiss Managing Director ISA99 made a presentation on **ISA, IEEE and Cybersecurity … the Need for Collaboration**
        i. Joe explained the reasons for the need to coordinate between ISA and IEEE Power Systems:
            1. Reduce overlap of product development
            2. Minimize inconsistency between standards
            3. Difference between the ISO 7 level communications model vs the Purdue reference model.
            4. ISA and IEEE has common equipment with common vendors.

5. Concern for Industrial Control Systems is the Level 0 & 1 (sensors and process bus) information is unprotected.
6. The collaboration between ISA99/IEC62443 and S0 work falls within S1 IEEE 1686 and S5 IEEE C37.240. Steve and Marc Lacroix will discuss how to liaison with Joe.

b. Didier Giarrantano – Liaison to IEC System Committee for Smartgrid explained how there is a need for mapping between IEC and IEEE PSCC. How do we liaison between the two organizations? Didier will give a presentation at the May S0 meeting.

c. New Study Groups to explore:

i. A core theme from the IEEE Cybersecurity workshop was the utility need for IT and OT collaboration to address cybersecurity differences (culture, application, perspective and terminology)
Study Group Assignment: Assess the IT-OT challenge in Utility Cybersecurity roles. Determine if a Task Force is required to create a report to assist in building organizational understanding and collaboration.

Steve is recommending a study group meet in May to determine if a task force should be created on the need for OT and IT collaboration would be beneficial. Steve and Brian Smith agreed to run this SG for May and report back to S0.

ii. Small utility/coop need a summarization of all cybersecurity standards and their relevance.
Study Group Assignment: Assess the challenge in utilities & municipalities with limited resources on the applicability and relevance of the cybersecurity standards. Determine if a Task Force is required to create a report to assist summarizing the relevant cybersecurity standards.

Steve is recommended a study group meet in May to determine if a task force should be created on the need to develop a cybersecurity standards summarization for small entities. Nathan

Wallace and James Formea agreed to run this SG in May and report back to S0.

7. Announcements:
    a. Group Minutes (will be posted online)
        i. Summary minutes to be provided to SC officers after your group meeting.
        ii. Detailed minutes to be provided to SC officers within 2 weeks after your group meeting.
    b. IEEE General Meeting has a slot for PSCC panel session (2 or 4 hours). Deadline for abstract submission is required by January 15th.
8. Meeting Adjourned

Addendums

Addendum 1: Working Group/Study Group/Task Force Summary / Status (details in group minutes)

WG S1: 1686 IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities **Chair:** Marc Lacroix **Vice-chair:** Éric Thibodeau **Scope:** The standard defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate cybersecurity programs. The standard addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an IED. Confidentiality, integrity and availability of external interfaces of the IED is also addressed. **Status:** PAR was approved and the WG met to start the revision of IEEE 1686.
WG S2: P1711.1 Serial SCADA Protection Protocol (SSPP) **Chair:** Ed Cenzon **Scope:** This standard defines the Substation Serial Protection Protocol (SSPP), a cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of substation serial links. It does not address specific applications or hardware implementations, and is independent of the underlying communications protocol. **Status:** Working Group did not meet in Jacksonville. Draft standard is being finalized and proceed to MEC review. WG vote and proceed to ballot. Plan is to be in ballot resolution by January 2018. WG PAR was extended to Dec 2018.
WG S3: P2030.102.1 Standard for Interoperability of IPSEC Utilized within Utility Control Systems **Chair:** Jim Bougie **Vice-chair:** Marc Lacroix **Secretary:** James Formea **Scope:** This standard specifies requirements for interoperability of devices utilized within utility control systems which implement the Internet Protocol Security (IPsec) protocol suite within an IPv4 environment.

Status: Group met to review open comments. WG PAR was extended to Dec 2018.

WG S4: P1711.2 Trial-Use Standard for Secure SCADA Communications Protocol (SSCP)

Chair: Mark Hadley

Scope: This trial use standard defines a cryptographic protocol to provide integrity with optional confidentiality for cyber security of substation serial links. It does not address specific applications or hardware implementations and is independent of the underlying communications protocol.

Status: Working Group did not meet in Jacksonville. Draft standard is being finalized to proceed for MEC review. WG PAR was extended to Dec 2018.

WG S5: Cybersecurity Requirements for Power System Automation, Protection and Control Systems

Chair: Steve Kunsman **Vice-chair:** TW Cease

Scope: Revision of IEEE C37.240 to included new technical requirements for power system cyber security. Based on sound engineering practices, requirements can be applied to achieve high levels of cyber security of automation, protection and control systems independent of voltage level or criticality of cyber assets.

Status: WG PAR was approved allowing the group to meet. The identified gaps were discussed and assignments made to begin drafting work. TW Cease has volunteered to be WG Vice-chair.

TF S6: IoT for connected home - Communication and cybersecurity requirements

Chair: Marc Lacroix **Vice-chair:** James Formea
Scope: To produce a report that describes the different use cases that make use of the Connected Homes concept, presents a security risk analysis and propose requirements for telecommunication (Volume, frequency, speed) and cybersecurity. Guidelines for utilities experts will be listed.

Status: Task Force has started work on producing the report. James Formea has been appointed as vice-chair.

TF S7: Electrical Power System Cyber Device Function Numbers, Acronyms, and Designations

Chair: Nathan Wallace
Scope: This task force explores the need for and creation of cyber device function numbers, acronyms, and designations for cyber devices and functions used in electrical power systems. This work focuses on identifying and providing a means for documenting enabled cyber related services and cybersecurity functions and measures.

Status: TF met to discuss the concept and creation of the report or standard.

TF S8: Testing Power System Cybersecurity Controls
Chair: Nathan Wallace
Scope: This task force explores the need for and creation of policies and procedures for the testing and commissioning of cybersecurity controls and measures used in electrical power systems.
Status: TF met to discuss the scope and PAR and decided to proceed to SC vote to move to a WG to develop a standard.

Addendum 2: TF S8 Par to be submitted at the S Sub-committee meeting on January 11th 2018

IEEE Guide for Cybersecurity Testing in Electric Power Systems

1. Overview

1.1 Scope

This document provides test guidance for cybersecurity controls used in electric power systems. The guide encompasses testing and verification of cybersecurity services, applications, and controls, including end-to-end testing.

1.2 Purpose

The transition to computational and communication assets in power systems brings with the need to verify cybersecurity controls are implemented and functioning properly.

1.3 Reason

Cybersecurity is one of the major concern for the power industry and utilities have to implement a security program to protect digital assets, including Protection & Control systems, that follow so-called best or common practices from the IT industry. A challenge, however, is the implementation and the subsequent verification of these cybersecurity approaches when applied to electric power systems. The nuances and priorities of the operational power system are unlike that of other environments and therefore guidance is needed that outlines the procedures and techniques associated with testing and verifying cybersecurity controls in power systems. This includes testing guidance associated with cybersecurity function testing, commissioning, maintaining, and troubleshooting devices and systems. In the case of commission testing, such cybersecurity testing and verification guidance can be used to help confirm adherence with a specified design philosophy and that the operational requirements are met. Stakeholders for the work include:

- Utilities/users who own the asset or have the daily responsibility of operating the assets and systems
- System integrators with the responsibility of ensuring that the operational expectations and requirements are being met.
- Security service providers with the responsibility of providing remote cybersecurity monitoring.
- Vendors
- Independent cybersecurity researchers and firms testing cybersecurity controls
- Regulatory agencies and government who have a vested interest in critical infrastructure protection program effectiveness.

1.4 Contact Information

Chair:

Nathan Wallace

n.wallace.us@ieee.org

Vice-Chair:

Deepak Maragal

Addendum 3: May 2018 S0 Subcommittee Meeting Requirements

WG S1: 1686 IEEE Standard for Intelligent Electronic Devices Cybersecurity Capabilities **Chair:** Marc Lacroix **Vice-chair:** Éric Thibodeau May Meeting requirements: Room for 20 people and a computer projector
WG S2: P1711.1 Serial SCADA Protection Protocol (SSPP) **Chair:** Ed Cenzon May Meeting requirements: Room for 20 people and a computer projector
WG S3: P2030.102.1 Standard for Interoperability of IPSEC Utilized within Utility Control Systems **Chair:** Jim Bougie **Vice-chair:** Marc Lacroix **Secretary:** James Formea May Meeting requirements: Room for 30 people and a computer projector
WG S4: P1711.2 Trial-Use Standard for Secure SCADA Communications Protocol (SSCP) **Chair:** Mark Hadley May Meeting requirements: Room for 20 people and a computer projector
WG S5: Cyber Security Requirements for Power System Automation, Protection and Control Systems **Chair:** Steve Kunsman **Vice-chair:** TW Cease May Meeting requirements: Room for 40 people and a computer projector
TF S6: IoT for connected home - Communication and cybersecurity requirements **Chair:** Marc Lacroix **Vice-chair:** James Formea May Meeting requirements: Room for 30 people and a computer projector
TF S7: Electrical Power System Cyber Device Function Numbers, Acronyms, and Designations **Chair:** Nathan Wallace May Meeting requirements: Room for 20 people and a computer projector
TF S8: Testing Power System Cybersecurity Controls **Chair:** Nathan Wallace May Meeting requirements: Room for 30 people and a computer projector
Demo S2: Study Group on P1711 and SSP21 California Energy Systems for the 21st Century (CES21) protocol comparison / Livermore national lab demonstration **Chair:** Scott Mix / Mark Hadley May Meeting requirements: Room for 30 people and a computer projector
SG S9: Study Group on Utility IT-OT Cybersecurity challenges in roles and terminology **Chair:** Steve Kunsman / Brian Smith May Meeting requirements: Room for 30 people and a computer projector
SG S10: Study Group on Utility & municipality challenges on understanding cybersecurity standards **Chair:** Nathan Wallace / James Formea May Meeting requirements: Room for 30 people and a computer projector