IEEE PSCC S5 WG: Extensions to Cyber Security requirements for Power System P&C, Automation systems

Chair: Steven Kunsman
Vice Chair: TW Cease
Output: Revision of Standard IEEE C37.240
Established: 7-Dec-2017
PAR Deadline: 31-Dec-2021

Summary Minutes for Subcommittee Report

The S5 WG meeting was held on Monday, January 8, 2018 with 19 attendees (16 of 21 members & 3 guest).

Purpose of S5 WG:

To review the gaps in IEEE C37.240-2014 "**Cybersecurity Requirements for Substation Automation, Protection and Control Systems"** and revise the existing standard.

Bring the industry experts together with power system domain knowledge and involved in the development of cyber security standardization and review the published IEEE C37.240 standard related to areas not addressed:

- Cyber security requirements for communications outside the control house but inside the substation fence
- H22 Guide for Cyber Security for Protection Related Data Files
- Cyber security for protection systems outside of the substation (Feeder automation/Wide area systems)
- Cyber security requirements for wireless applications
- Application Whitelisting and Blacklisting including Communication Whitelisting
- Usage and Management of Digital Signatures
- Cloud based application
- C37.240 audit support documentation
- Reference appendix to map the standard into NERC CIP applications

The proposed PAR was discussed, revised and approved by the attendees. Some of the gaps identified to be addressed in the revision were reviewed to build knowhow in the group (see supporting power point pdf)

Request for May 2018 S5 plans to meet as a Working Group in a single session for 50 people and a computer projector.

PSCC S5 Extensions other Cyber Security Requirements for Substation P&C Systems

Agenda

1. **Introductions**
2. **IEEE Call for Patents/IP**
3. **Approval of September 2017 Task Force Minutes**
   Approval of September was not conducted as the Task Force moved to the WG.
4. **Status of PAR** – we reviewed the approved PAR and the single change required by NESCOM.
5. **Identified Gap Dialog (Writing Assignments)**
   a. **Cyber security requirements for communications outside the control house but inside the substation fence** – Steve Kunsman, Farel Becker, Herb Falk, Jay Anderson, James Formea
   b. **H22 Guide for Cyber Security for Protection Related Data Files** – Tony Johnson, TW Cease, Dennis Holstein
   c. **Cyber security for protection systems outside of the substation** (Feeder automation/Wide area systems) – Ryan Newell, Chris Huntley, Mital Kanabar, Xiangyu Ding, Peter Rietmann
   d. **Cyber security requirements for wireless applications**. There was an in depth discussion on the wireless topic. There are two aspects to wireless (physical and data) and ISA 100 would be a good starting point to review. The focus should be on How to assess the cybersecurity requirements for wireless. – Craig Preuss, Marc Lacroix, Dennis Holstein
   e. **Application Whitelisting and Blacklisting** including Communication Whitelisting – Herb Falk, Craig Preuss, Mark Lacroix
   f. **Applications and Management of Digital Signatures** – Herb Falk, James Formea, Didier Giarrantano
   g. **Cloud based application** – Farel Becker, Dennis Holstein
   h. **C37.240 audit support documentation** (also to review IEC 62443-2.4 for auditing– Tony Johnson, Jay Anderson
   i. **Reference appendix to map the standard into NERC CIP applications** – Tony Johnson, Scott Mix

6. **Next Steps**
   a. Requested Erin S from IEEE for C37.240-2014 document and translation to new IEEE standard template.

b. Requested Erin S from IEEE for associated standards.