

## **IEEE PSCC S5 TF: Extensions to Cyber Security requirements for substation P&C systems**

**Chair: Steven Kunsman**

**Vice Chair: Chan Wong**

**Output: Task Force recommendation to proceed as a working group and submit PAR**

**Established: May 2016**

### **Summary Minutes for Subcommittee Report**

The S5 TF meeting was held on Monday, September 11, 2017 with 16 attendees (7 members & 9 guest).

#### **Purpose of S5 TF:**

To review the gaps in IEEE C37.240 “**Cybersecurity Requirements for Substation Automation, Protection and Control Systems**” and decide if a WG should be formed to amend or 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 Jan 2015 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 usage 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 January 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**

- 1. Agenda**
- 2. Introductions**

Approval of May meetings notes-approved and seconded by several members

- 3. Purpose of this Task force and working group-** It was discussed that one of the main purposes of this Task Force- is to bring IT and OT for the substation on the same page.

Revision C37.240 PAR – the PAR is being reviewed this month and anticipated to be approved and then a working group will be formed and moving forward in January 2018

**Group Question-**Does the document define what a cyber asset. Per Craig-not is not document, but is found in the NERC CIP standard and IEEE dictionary.

**Group Question-**Does this document include RAS? Steve said it could as long as it not on requirements for application which are the responsibility of H the subcommittee.

**Group Question** from Craig-should the PAR title have Cyber Security as one word to try and capture the Physical security as well.

**Group Question** what is the definition of the “high Level” Cyber Security- Steve stated there is no such thing as 100% secure.

#### 4. Need for the project?

**Group Question**-What is the long-term time horizon for the process bus.

- Other things that could be discussed in the project
  - **Cyber Security requirements for outside the control house? No longer a 6 wall constraint via NERC CIP**
    - Why do we want to have routable protocol inside the substation fence?
      - Asset monitoring
      - Process Bus
        - Only requires a strong password
      - Wireless outside the Substation
        - Feeder Automation-reclosers
    - **Question**-is channel security included in the scope of this standard? Having ways to show how the communications may be protected against doing away with the 6 wall principal would be good to have as part of the standard to lay aside the concerns of the IT community.
    - Per Denise Holstein-62443 3-2 Security for industrial automation and control systems would be a good reference for this standard to defined the security zones.
  - **H22 -guide for protection and Automation related data files-Comment for Tony Johnson SCE**
  - This guide could
    - Support NERC CIP Audit Documentation
      - Key for helping the utility to prove to their auditor
    - Provide Guidelines for the use of Wireless applications
      - Could include:
        - WiMax, LTE 4G, Satellite, Microwave

**Group Question**-will multifactor access control be considered-Steve said yes, Denise Holstein cautioned about the work being done on Privacy data from various IEEE working group.

**Group Question**-what are the methods recommended by IEEE for White listing? CIGRE Study Committee D2 (691) would be a good reference.

What will the impact of the future Dark Grid be?

What is the timeline for this revision-Three years

#### **Need for project paragraph #2-Change:**

- **“Substation Applications” to “Power Systems Applications”**
- **“Protection systems” “Protection Automation Control Systems”**
- **Change the word Cyber Security to one word.**

PAR should be in by 10/26 and approved by 10/31.