IEEE PSCC S1 SG: IEEE 1686 Standard for Intelligent Electronic Devices Cyber Security Capabilities

Chair: Marc Lacroix
Vice Chair: Open
Output: New PAR for the revision of the standard
Established: May 2016

Summary Minutes for Subcommittee Report
The S1 SG meeting was held on Monday, Sept 11, 2017 with 22 attendees.
The goal of this meeting was to present the scope of the existing standard and discuss the opportunity of modifying it.

Purpose of S1 SG:
The task force will revise the existing IEEE 1686 standard to integrate the latest cybersecurity technologies in order to defines the functions and features to be provided in IEDs to support cybersecurity programs.

Request for Jan 2018 S1 plans to meet as a Task Force in a single session for 40 people and a computer projector.

Meeting started with task force Chair- Marc Lacroix introducing the purpose of the taskforce and with an overview of existing standard.
A vice-chair was nominated. Éric Thibodeau has accepted to take this responsibility.
There was a lot of discussions and the consensus is that the standard need to be revised.

Previous revision was aligned on publication of NERC CIP requirements. Again, new requirements were issued and call for a revision of 1686.

Opinions about need to revise the standard

- Need to revise requirements for use control. May need to go further than RBAC
- New elements may also fall under C37.240. Scope check for every new requirement.
- Requirements must not assume the presence of ESP/PSP because IEDs may be installed in the field
    - Section on security assumptions should be added because security requirements might change depending on assumptions. For example, port access monitoring might not me required if within a PSP.
    - On the other side, the goal of 1686 was only to provide a list of requirements, not to elaborate on the context of those requirements.
- Authentication: already addressed using local accounts; addition of central security (LDAP, RADIUS, etc.) might be desirable
- State-Based RBAC: privileges might change depending on the state of the device and their environment. Exceptional cases where override of access might be granted.
- Are network devices falling under IED definition? Must be clarified by the standard
- Should be open to extend outside substation devices
- Look where security is headed outside PS domain
- For example, passwords might not be future way to authenticate. Standard may look into other forms of authentication: certificates, bio, etc…
- Is the standard about CIP compliance or IED security? Should be both, with notes to point to CIP. Again, many more CIP programs than only NERC
- Data at rest on the IED itself. Might conflict with PSRC H22 scope?
- See the versions of open source software installed on device, to control known security holes

General consensus is that revision is required and a PAR should be open

Expected scope for future PAR was revised

Actions items

1) Marc Lacroix will prepare a PAR for the P0 committee.