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

Chair: Marc Lacroix
Vice Chair: Éric Thibodeau
Output: Revision of the standard
Established: Dec 2017

Summary Minutes for Subcommittee Report

The S1 WG meeting was held on Monday, January 14 with 26 attendees (13 members).

The goal of this meeting was to continue working on the revision of IEEE 1686 standard.

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 May 2019 S1 plans to meet as a Working Group in a single session for 40 people and a computer projector.

First edition of 1686 was made many years ago and has not changed much in its last revisions. It now needs a major overhaul to make it up to date with good practices. Will require to overhaul the outline

Since physical integrity is addressed in the draft, do we need to change the title of the standard? Instead of using cyber security in two words, the use of cybersecurity implies the physical security. This suggestion is approved. We will see in the future to update the PAR with the new title.

Reporting of events in the standard was meant to be reported via DNP3 or similar SCADA protocols. Clarify 5.2 by adding (events and alarms recording) to title and 5.3 by adding (events and alarms reporting)

James highlights the caution we must show in our use of the audit trail definition. We must be cautious in changing the title Audit trail to events and alarms recording. Manufacturers may have features called “audit trail” in their devices. Note must be added to the standard.

Discussion about “Supervisory permissive control” (5.3.6). Odd part of the standard. Consensus seems to be that this does not belong to cybersecurity and should be removed.

Suggestion to rename 5.1 Access Control to “Authentication”. The section will be renamed to “Authentication, Authorization and Access Control”

The section must make clear it addresses Machine-Machine interaction.

On 5.1.3, what to do if the device is hooked to a central managed account system? The number of supported users becomes a bit pointless. The way it is worded is confusing. To be corrected.

Different types of Authentication: Local Password Authentication, Centralized Password Authentication or Certificate Authentication. Each of these approaches must be included in the standard (at least the capability of the IED supporting the different authentication methods). When authenticated, then authorization and access control will be done, independently of the method of authentication.

Definition of IED should now encompass virtual devices also (verify what is defined in 61850). Suggestion: "… incorporating one or more processors, either physically dedicated or virtually allocated…"

Discussion about the possibility of updating security and communications features independently from core functionalities. This to avoid re-testing a whole device for every security patch. Still tests will be required, but will limit field re-test.

Contributions are needed for the four new sections of the standard, 5.8 to 5.11

Chain of Supply; use of open source is more and more widespread, number of libraries is increasing; All of these should be tracked and be trackable by customers to be able to address the potential vulnerabilities.

Actions items

1)