1. Project Number: P1686
2. Type of Document: Standard
3. Life Cycle: Full Use

1. Title: Standard for Intelligent Electronic Devices Cyber Security Capabilities

Changes in title: IEEE Standard for Intelligent Electronic Devices Cyber Security Capabilities

3.1 Working Group: Cybersecurity Subcommittee (PE/PSCC/S1-WG)

Contact Information for Working Group Chair
Name: Samuel Sciacca
Email Address: samuel.sciacca@ieee.org
Phone: 2037321716

Contact Information for Working Group Vice-Chair
None

3.2 Sponsoring Society and Committee: IEEE Power and Energy Society/Power System Communications and Cybersecurity (PE/PSCC)

Contact Information for Sponsor Chair
Name: Daniel Nordell
Email Address: d.nordell@ieee.org
Phone: 612-630-4422

Contact Information for Standards Representative
Name: Michael Dood
Email Address: mdood@ieee.org
Phone: 509-336-7133

4. Type of Ballot: Individual

4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 06/2019

4.3 Projected Completion Date for Submittal to RevCom
Note: Usual minimum time between initial sponsor ballot and submission to Revcom is 6 months.: 02/2020

5. Approximate number of people expected to be actively involved in the development of this project: 20

Changes in scope: The standard defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate critical infrastructure protection (CIP) programs. The standard addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an IED. Encryption of communications and availability of external interfaces of the IED is also addressed.

5.3 Is the completion of this standard dependent upon the completion of another standard: No

Changes in purpose: The standard defines the functions and features to be provided in IEDs to support cybersecurity programs. Specifically, the standard states what safeguards, audit mechanisms and alarm indications shall be provided by the vendor of the IED with regard to all activities associated with access, operation, configuration, firmware revision and data retrieval from an IED. The standard also allows the user to define a security program around these features, and alert the user if an IED does not meet this standard as to the need for other...
defensive measures (technical and/or procedural) that may need to be taken. The encryption for the secure transmission of data both within and external to the IED secure perimeter is also part of this standard.

5.5 Need for the Project: Cybersecurity is one of the major concerns for the industry and utilities have to implement a security program to protect digital assets, including Protection & Control systems, that follows so-called "best practices" from the IT industry. The rationale is to protect the bulk power delivery system from compromise and guard utilities against embarrassment, loss of revenue and potential litigation caused by customer interruption from security breaches.

The industry must also follow the rules prescribed by the North American Electric Reliability Corporation (NERC) in a series of cyber security standards for critical infrastructure protection (CIP) which, depending on the CIP program at a utility, may drive requirements for cyber security features in some IEDs. The standard will include a table that includes correspondence between 1686 and CIP requirements.

Stakeholders for the project are:
- Utilities/users who can specify that IEDs meet this standard to be consistent with their cybersecurity programs
- Vendors who will have a clear understanding of the functions and features that must be present in their product offerings
- Regulatory agencies and government who have a vested interest in critical infrastructure protection program effectiveness

5.6 Stakeholders for the Standard: 1. Utilities/Users - Purchasers of substation IEDs.
2. IED Vendors
3. Regulatory Agencies - Agencies and government organizations with an interest in utility CIP such as NERC, FERC, DHS and DOE.

Intellectual Property

6.1.a. Is the Sponsor aware of any copyright permissions needed for this project?: No
6.1.b. Is the Sponsor aware of possible registration activity related to this project?: No

7.1 Are there other standards or projects with a similar scope?: No
7.2 Joint Development

Is it the intent to develop this document jointly with another organization?: No

8.1 Additional Explanatory Notes: This standard was originally sponsored by substation committee.

It is now under the responsibility of Power System Communications and Cybersecurity Committee.