Smart Grid Interoperability Panel (SGIP) Cyber Security Working Group (CSWG) Standards Review

CSWG Standards Review Report

IEEE 1686 Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

October, 2011

Security Assessment of IEEE 1686 Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

1. Introduction

1.1 Correlation of Cybersecurity with Information Exchange Standards

Correlating cybersecurity with specific information exchange standards, including functional requirements standards, object modeling standards, and communication standards, is very complex. There is rarely a one-to-one correlation, with more often a one-to-many or many-to-one correspondence.

First, communication standards for the Smart Grid are designed to meet many different requirements at many different "layers" in the communications "stack" or "profile." One example of such a profile is the GridWise Architecture Council (GWAC) Stack. Some standards address the lower layers of the communications stack, such as wireless media, fiber optic cables, and power line carrier. Others address the "transport" layers for getting messages from one location to another. Still others cover the "application" layers, the semantic structures of the information as it is transmitted between software applications. In addition, there are communication standards that are strictly abstract models of information – the relationships of pieces of information with each other. Since they are abstract, cybersecurity technologies cannot be linked to them until they are translated into "bits and bytes" by mapping them to one of the semantic structures. Above the communications standards are other security standards that address business processes and the policies of the organization and regulatory authorities.

Second, regardless of what communications standards are used, cybersecurity must address all layers – end-to-end – from the source of the data to the ultimate destination of the data. In addition, cybersecurity must address those aspects outside of the communications system in the upper GWAC Stack layers that may just be functional requirements or may rely on procedures rather than technologies, such as authenticating the users and software applications, and screening personnel. Cybersecurity must also address how to: cope during an attack, recover from it afterwards, and create a trail of forensic information to be used in post-attack analysis.

Third, the cybersecurity requirements must reflect the environment where a standard is implemented rather than the standard itself: how and where a standard is used must establish the levels and types of cybersecurity needed. Communications standards do not address the importance of specific data or how it might be used in systems; these standards only address how to exchange the data. Standards related to the upper layers of the GWAC Stack may address issues of data importance.

Fourth, some standards do not mandate their provisions using "shall" statements, but rather use statements such as "should," "may," or "could." Some standards also define their provisions as being "normative" or "informative." Normative provisions often are expressed with "shall" statements. Various standards organizations use different terms (e.g., standard, guideline) to characterize their standards according to the kinds of statements used. If standards include security provisions, they need to be understood in the context of the "shall," "should," "may," and/or "could" statements, "normative," or "informative" language with which they are expressed.

Therefore, cybersecurity must be viewed as a stack or "profile" of different security technologies and procedures, woven together to meet the security requirements of a particular implementation of a stack of policy, procedural, and communication standards designed to provide specific services. Ultimately, cybersecurity as applied to the information exchange standards should be described as profiles of technologies and procedures which can include both "power system" methods (e.g. redundant equipment, analysis of power system data, and validation of power system states) and information technology (IT) methods (e.g. encryption, role-based access control, and intrusion detection).

There also can be a relationship between certain communication standards and correlated cybersecurity technologies. For instance, if TCP/IP is being used at the transport layer and if authentication, data integrity, and/or confidentiality are important, then TLS (transport layer security) should most likely (but not absolutely) be used.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be taken into account.

1.2 Correlation of Cybersecurity Requirements with Physical Security Requirements

Correlating cybersecurity requirements with specific physical security requirements is very complex since they generally address very different aspects of a system. Although both cyber and physical security requirements seek to prevent or deter deliberate or inadvertent attackers from accessing a protected facility, resource, or information, physical security solutions and procedures are vastly different from cybersecurity solutions and procedures, and involve very different expertise. Each may, in fact, be used to help protect the other, while compromises of one can definitely compromise the other.

Physical and environmental security that encompasses protection of physical assets from damage is addressed by the NISTIR 7628 only at a high level. Therefore, assessments of standards that cover these non-cyber issues must necessarily also be at a general level.

1.3 Standardization Cycles of Information Exchange Standards

Information exchange standards, regardless of the standards organization, are developed over a time period of many months by experts who are trying to meet a specific need. In most cases, these experts are expected to revisit standards every five years in order to determine if updates are needed. In particular, since cybersecurity requirements were often not included in standards in the past, existing communication standards often have no references to security except in generalities, using language such as "appropriate security technologies and procedures should be implemented."

With the advent of the Smart Grid, cybersecurity has become increasingly important within the utility sector. However, since the development cycles of communication standards and cybersecurity standards are usually independent of each other, appropriate normative references between these two types of standards are often missing. Over time, these missing normative references can be added, as appropriate.

Since technologies (including cybersecurity technologies) are rapidly changing to meet increasing new and more powerful threats, some cybersecurity standards can be out-of-date by the time they are released. This means that some requirements in a security standard may be inadequate (due to new technology developments), while references to other security standards may be obsolete. This rapid improving of technologies and obsolescence of older technologies is impossible to avoid, but may be ameliorated by indicating minimum requirements and urging fuller compliance to new technologies as these are proven.

1.4 References and Terminology

References to the National Institute of Standards and Technology (NIST) security requirements refer to the NIST Interagency Report (IR) 7628, *Guidelines to Smart Grid Cyber Security*, Chapter 3, High-Level Security Requirements.

References to "government-approved cryptography" refer to the list of approved cryptography suites identified in Chapter 4, Cryptography and Key Management, of NISTIR 7628. Summary tables of the approved cryptography suites are provided in Chapter 4.3.2.1.

The terms "approved", "acceptable", and "deprecated" are defined as the following[1]:

[1] The definitions are obtained from NIST Special Publication 800-131A, Transitions: *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*

- Approved is used to mean that an algorithm is specified in a FIPS or NIST Recommendation (published as a NIST Special Publication).
- Acceptable is used to mean that the algorithm and key length is safe to use; no security risk is currently known.
- Deprecated means that the use of the algorithm and key length is allowed, but the user must accept some risk. The term is used when discussing the key lengths or algorithms that may be used to apply cryptographic protection to data (e.g., encrypting or generating a digital signature).

As noted, standards have different degrees for expressing requirements, and the security requirements must match these degrees. For these standards assessments, the following terminology is used to express these different degrees[2]:

- Requirements are expressed by "…shall…," which indicates mandatory requirements strictly to be followed in order to conform to the standard and from which no deviation is permitted (*shall* equals *is required to*).
- Recommendations are expressed by "…should…," which indicates that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others; or that a certain course of action is preferred but not necessarily required (*should* equals *is recommended that*).
- Permitted or allowed items are expressed by "…may…," which is used to indicate a course of action permissible within the limits of the standard (*may* equals *is permitted to*).
- Ability to carry out an action is expressed by "…can …," which is used for statements of possibility and capability, whether material, physical, or causal (*can* equals *is able to*).
- The use of the word *must* is deprecated, and should not be used in these standards to define mandatory requirements. The word *must* is only used to describe unavoidable situations (e.g. "All traffic in this lane must turn right at the next intersection.")

2. IEEE 1686 Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities

2.1 Description of Document

The IEEE 1686, *Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities,* defines the cybersecurity functions and features to be provided in substation 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.

The focus of the cybersecurity requirements is in interfaces between users and IEDs, including user direct access, audit logs, and user access through supervisory control and data acquisition (SCADA) systems.

2.2 Assumptions

This standard addresses IEDs within a substation environment, which assumes physical access protection is provided by the substation walls and control house. Encryption for the secure transmission of data within and external to the substation, including SCADA, is not part of this standard and addressed in other efforts.

[2] The first clause of each terminology definition comes from the International Electrotechnical Commission (IEC) Annex H of Part 2 of ISO/IEC Directives. The second clause (after "which") comes from the Institute of Electrical and Electronics Engineers (IEEE) as a further amplification of the term.

2.3 Assessment of Cybersecurity Content

2.3.1 Does the standard address cybersecurity? If not, should it?

IEEE 1686 addresses the functions and features to be provided in substation IEDs to accommodate CIP programs, including security regarding the access operation, configuration, firmware revision, and data retrieval from an IED.

2.3.2 What aspects of cybersecurity does the standard address and how well (correctly) does it do so?

Table 1: Correlations between Standard being Assessed and the NISTIR Security Requirements

Reference in Standard	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.1 Electronic access control	SG.AC-4 Access Enforcement	
5.1.1 Password defeat mechanisms	SG.AC-14 Permitted Actions without Identification or Authentication	
5.1.2 Number of individual ID/passwords supported	SG.AC-3 Account Management	The minimum number of unique user-access ID/passwords are mandated, but no requirements are included for specifying the types of accounts.
5.1.3 Password construction	SG.AC-21 Passwords	A minimum password length (8 characters) is required; however, strong authentication and changing passwords are not addressed.
5.1.4 Authorization levels by password	SG.AC-6 Separation of Duties SG.AC-7 Least Privilege	This requirement allows assignment of one or more access capabilities to ID/password accounts, although it does not explicitly acknowledge the concept of separation of duties or least privilege. The rationale is if functionality could be assigned individually by associating each password with its list of allowed functions, then a greater granularity of assignment could be achieved.
5.1.4.2 View configuration settings	SG.CM-5 Access Restrictions for Configuration Change	
5.1.4.3 Force values	SG.CM-5 Access Restrictions for Configuration Change SG.SI-7 Software and Information Integrity	By restricting access to the ability to "force values" (manually override real data with manually inputted data), some protection is provided to the integrity of information by limiting who can force data, but this protection is only applicable to forcing values. Validation of input data is not included.
5.1.4.4 Configuration change	SG.CM-5 Access Restrictions for Configuration Change	
5.1.4.5 Firmware change	SG.CM-5 Access Restrictions for Configuration Change	
5.1.4.6 ID/password management	SG.AC-3 Account Management	

Reference in Standard	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.1.5 Password display	SG.IA-6 Authenticator Feedback	
5.1.6 Access time-out	SG.AC-13 Remote Session Termination	
5.2 Audit trail	SG.AU Audit and Accountability Policy and Procedures	
5.2.1 Storage capability	SG.AU-4 Audit Storage Capacity	
5.2.2 Storage record	SG.AU-3 Contents of Audit Records	
5.2.3 Audit trail event types	SG.AU-2 Auditable Events SG.CM-4 Monitoring Configuration Changes	The section lists the types of events that must be audited, including configuration changes. However, the list should be updated to include: • Return of forced values to monitored values; • Deletion or modification of any audit log entries; • Pending overflow of audit log; • Communication failures and restarts; and • Automated time corrections greater than normal variations.
5.3 Supervisory monitoring and control	SG.SI-4 Smart Grid Information System Monitoring Tools and Techniques SG.IR-6 Incident Monitoring	
5.3.5 Supervisory permissive control	SG.AC-15 Remote Access	The requirement is for supervisory access control (supervisory permission) before a control command is issued to power system equipment. This requirement is not explicitly covered in the NISTIR 7628.
5.4 Configuration software	SG.SI-7 Software and Information Integrity SG.CM-7 Configuration for Least Functionality	
5.4.1 Authentication	SG.CM-5 Access Restrictions for Configuration Change	
5.4.2 ID/password control	SG.CM-5 Access Restrictions for Configuration Change	
5.4.3 ID/password-controlled features	SG.CM-5 Access Restrictions for Configuration Change	
5.5 Communications port access	SG.CM-7 Configuration for Least Functionality	Ports must be capable of being enabled or disabled, but are not required to be disabled if not necessary for functionality. This does not meet the NISTIR 7628 security requirement, SG.CM-7.

Reference in Standard	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.6 Firmware quality assurance	SG.MA Smart Grid System Development and Maintenance	The requirements refer to IEEE C37.231, which has not been formally reviewed as part of the assessment of IEEE 1686. However, an informal review of C37.231 found the coverage of cybersecurity in that document to be inadequate. This review will need to be verified.

2.3.3 What aspects of cybersecurity does the standard not address? Which of these aspects should it address? Which should be handled by other means?

Although the IEEE 1686 standard addresses cybersecurity requirements for user interactions with IEDs, it does not address other key cybersecurity issues related to these IED requirements such as:

- Inter-IED interactions;
- SCADA-IED interactions, except for supervisory access control and other remote access to field devices;
- Encryption requirements, such as referencing the NIST-sanctioned cryptographic suites;
- IED continuity of operations;
- IED disaster recovery;
- Teleprotection interactions;
- IEDs outside of substations;
- Provision for strong authentication; and
- Better coverage of patch management and related cybersecurity.

2.3.4 What work, if any, is being done currently or is planned to address the gaps identified above? Is there a stated timeframe for completion of these planned modifications?

IEEE 1686 is currently being updated. An IEEE Project Authorization Request (PAR) was approved in September 2011, with expected Sponsor Balloting in December 2012. In this update, the reference to "substation" has been removed to allow the document to be applied to IEDs in other utility environments. This updated standard will not address physical security, but is expected to address additional IED issues. Additional participation in the IEEE 1686 update effort is welcome[3].

Recent and ongoing work on revision of other relevant standards will also facilitate the remediation of gaps identified in IEEE 1686. A document identifying some of these other efforts is located under the CSWG comments section on the SGIP IEEE 1686 Twiki web page at http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCosSIFIEEE16862007.

2.3.5 Recommendations

The CSWG recommends that the comments in Table 1 and issues described in Section 2.3.3. be addressed in the updated version of IEEE 1686.

[3] http://www.pestechnical.org/2011/Schedule.asp?CID=2

2.3.6 List any references to other standards and whether they are normative or informative

2.3.6.1 Normative

- IEEE Std C37.231™, IEEE Recommended Practice for Microprocessor-Based Protection Equipment Firmware Control.

2.3.6.2 Informative

- Accredited Standards Committee C2-2007, National Electrical Safety Code® (NESC®).4
- IEEE PC37.1™ (D5, Sept. 2007), IEEE Draft Standard for SCADA and Automation Systems. 5, 6, 7
- IEEE PSRC Working Group Report, "Cyber Security Issues for Protective Relays."
- NERC CIP 002-1, Cyber Security—Critical Cyber Asset Identification.8
- NERC CIP-003-1, Cyber Security—Security Management Controls.
- NERC CIP-004-1, Cyber Security—Personnel and Training.
- NERC CIP-005-1, Cyber Security—Electronic Security Perimeter(s).
- NERC CIP-006-1, Cyber Security—Physical Security of Critical Cyber Assets.
- NERC CIP-007-1, Cyber Security—Systems Security Management.
- NERC CIP-008-1, Cyber Security—Incident Reporting and Response Planning.
- NERC CIP-009-1, Cyber Security—Recovery Plans for Critical Cyber Assets.
- IETF RFC 1157, Simple Network Management Protocol (SNMP)