Smart Grid Interoperability Panel (SGIP)

Cyber Security Working Group (CSWG)

Standards Review

CSWG Standards Review Report

SGIP Priority Action Plan 13

Draft Standard Profile for Use of IEEE Std. 1588 Precision Time Protocol in Power System Applications IEEE PC37.238™/D5.7

April 28, 2011

Security Assessment of PAP13: Draft Standard Profile for Use of IEEE Std. 1588 Precision Time Protocol in Power System Applications IEEE PC37.238™/D5.7

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.

Secondly, 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.

Thirdly, 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.

Fourthly, 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 are taken into account.

1.2 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.

1.3 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.

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[1]:

- 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. Guidelines for Assessing Wireless Standards for Smart Grid Applications

2.1 Description of Document

"This standard specifies a common profile for use of IEEE 1588-2008 Precision Time Protocol (PTP) in power system protection, control, automation and data communication applications utilizing an Ethernet communications architecture.

In addition to distributing global time that is traceable to a recognized standard time source, the profile has a provision for distributing local time for the cases when connectivity to recognized standard time sources is lost.

The profile can be used for precise time synchronization of the devices in a substation, and between substations in a larger geographical area, if performance requirements of this standard are met.

The use of different physical layer communication technologies to carry Ethernet frames, including SONET/SDH and wireless technologies, is not precluded if they can meet performance requirements of this standard.

[1] 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.

Time distribution specified in this standard is based on the following basic assumptions:

- *all devices that participate in time distribution support this standard*
- *all devices are in the same time distribution domain*
- *all devices have point-to-point connections to their neighbors*
- *transmit and receive cable delay for each point-to-point connection is symmetrical*
- *known asymmetry in cable delay can be configured and corrected*

The use of security techniques is an important consideration; and, based on the application may be desirable or mandated. Security extensions and network engineering methods for hardening the PTP-based time distribution system against malicious attacks are not covered, and are outside of scope of this standard. If security techniques are used, they should not impair the ability of devices to achieve performance, specified in this standard.

Redundancy is an important consideration; some applications recommend or mandate support for different time distribution technologies, e.g. GPS and IRIG-B. Support for multiple time distribution technologies at the same time is out of scope of this standard."

2.2 Assumptions

IEEE PC37.238 is a profile of a well-defined subset of IEEE 1588-2008 mechanisms and settings aimed at enabling device interoperability, robust response to network failures, and deterministic control of delivered time quality over an Ethernet-based communications architecture.

Because of this relationship, all of the actual requirements specifications are defined in IEEE 1588-2008, not in this profile document.

2.3 Assessment of Cybersecurity Content

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

IEEE PC37.238 addresses security by referencing IEEE 1588-2008, as well as indicating some security-related best practices. The introduction to IEEE PC37.228 identifies the importance of security put indicates that it is outside the scope of the standard.

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

The correlations between this document and the security requirements described in NISTIR 7628's Chapter 3, families and requirements, are shown in Table 1 below.

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

Reference in Standard[2]	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement is Not Completely Met
5.4.2 Default settings	SG.AC-2 Remote Access Policy and Procedures	*"Slave-only clocks shall not transmit IEEE C37.238 Announce messages, in order to avoid advertising themselves as potential grandmasters."* This statement, although a remote access policy, seems to imply that if a slave-only clock did send an Announce message, it could be mistaken for a grandmaster.
5.5 Management Mechanism	SG.SC-20 Message Authenticity	*"All grandmaster-capable devices shall report TimeQuality and traceability to a recognized standard time source."* Although not a message authenticity per se, this provides authentication to the device.
5.6 Transport Mechanism	SG.SC-20 Message Authenticity	*"By default, all devices shall accept IEEE C37.238 messages that have had their IEEE Std 802.1Q tags removed, and tagged IEEE C37.238 messages with any VID value.* *Note: IEEE Std 802.1Q tags are often removed at bridge edge ports."* The IEEE group should review these statements and amend them if applicable.
C.1 Time performance parameters	SG.SC-5 Denial-of-Service Protection	*"Slave clocks may need to track the performance of their parent in order to determine whether the parent's signal is a valid signal, as required by Annex A.4 of IEEE Std 1588-2008. Remote substations utilizing PTP may be subject to grandmaster clock failure when time or frequency can become incorrect, plus deliberate effects such as GPS spoofing that substitutes the real GPS signals with other signals.* *Mechanisms to provide this performance monitoring may be considered in a future revision of the IEEE Std C37.238"* Although the potential for denial of service (lack of accurate clock source) is recognized, there is no specific technological specification on how to mitigate the problem.
D.3 Use of received IEEE C37.238 Announce messages to determine the time's quality	SG.SC-8 Communication Integrity	Message validation requirements for time traceability, quality, and source of clock time.
Annex F Management Information Base	SG.SC-8 Communication Integrity	Time traceability, quality, source of clock time, and other information is provided in an SNMP MIB

[2] The references may be just the section numbers or could include the title of the section

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?

The actual security techniques are covered in IEEE 1588-2008. IEEE PC37.238 is a profile document that defines a subset. However, the following have been identified as gaps:

- Security, as defined in IEEE 1588, is not required – it remains an option, as it is an included as an informative, experimental annex.
- Some vulnerabilities (as noted in the Table 1) are recognized, but no solutions or mitigating measures are provided.

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?

This document is still in draft form and will be updated.

2.3.5 Recommendations

In order to resolve the identified gaps, the CSWG recommends that:

- The IEEE group review the note on 802.1Q and revise the document as appropriate.
- This profile should explicitly include the security capabilities of IEEE 1588-2008 as mandatory, including discussions of known vulnerabilities.
- Best practices for additional end-to-end security should be developed to address vulnerabilities that could cause serious time-synchronization problems.

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

2.3.6.1 Normative References

- IEEE Std 1588™ – 2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems.

2.3.6.2 Informative References

- IEC 61850-5 Ed. 1.0 Communication networks and systems in substations – Part 5: Communication 5 requirements for functions and device models.
- IEC 61850-7-2 Ed. 2.0 Communication networks and systems in substations - Part 7-2: Basic communication structure for substation and feeder equipment – Abstract communication service interface (ACSI).
- IEC 61850-9-2 Ed. 2.0 (to be published) Communication networks and systems in substations – Part 9-2: Specific communication service mapping (SCSM) – Sampled values over ISO/IEC 8802-3.

- IEC 62439-3 Ed. 1.0 Industrial communication networks high availability automation networks - Part 3: Parallel Redundancy Protocol (PRP) and High availability Seamless Ring (HSR).
- IEEE Std 802.1Q-2005 IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks.
- IEEE Std C37.118-2005 IEEE Standard for Synchrophasors for Power Systems.
- International Vocabulary of Basic and General Terms in Metrology.
- ISO/IEC 10646:2003 Information technology - Universal Multiple-Octet Coded Character Set (UCS).
- PC37.118.2 / D1.1 Draft Standard for Synchrophasor Data Transfer for Power Systems
- IEEE Standards Interpretations for IEEE Std 1588™-2008, IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems. (http://standards.ieee.org/findstds/interps/1588-2008.html)