

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

CSWG Standards Review Report

*SmartGrid / AEIC AMI Interoperability
Standard Guidelines for ANSI C12.19 / IEEE
1377 / MC12.19 End Device Communications
and Supporting Enterprise Devices, Networks
and Related Accessories*

November 12, 2010

Security Assessment of SmartGrid/AEIC AMI Interoperability Standard Guidelines for ANSI C12.19 / IEEE 1377 / MC12.19 End Device Communications and Supporting Enterprise Devices, Networks and Related Accessories

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)¹ 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.

¹GridWise Architecture Council, http://www.gridwiseac.org/pdfs/interopframework_v1.pdf

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. For some specific Smart Grid communication standards, such as International Electrotechnical Commission (IEC) 61850 and IEC 60870-6, specific cybersecurity standards (IEC 62351 series) were developed to meet typical implementations of these standards.

In the following discussions of information exchange standard(s) being reviewed, these caveats should be 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 degrees²:

- 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. SmartGrid / AEIC AMI Interoperability Standard Guidelines for ANSI C12.19 / IEEE 1377 / MC12.19 End Device Communications and Supporting Enterprise Devices, Networks and Related Accessories

2.1 Description of Document

The SmartGrid / AEIC AMI Interoperability Standard identifies:

- The components of Enterprise semantics and object models defined by IEEE-P1377-2010 / ANSI C12.19-2008 / MC12.19-2010, and
- The required communication Application Services protocols provided by Standards such as IEEE P1703-2009 / ANSI C12.22-2008 / MC12.22-2010, IEEE P1701-2009 / ANSI C12.18-2006 / MC12.18-2010 and IEEE 1702- 2009 / ANSI C12.21-2006 / MC12.21-2010.

This document is intended for use as a voluntary guideline by all compliant Utility enterprise head-end systems, billing systems, interfaces to the metering network, meters and End Devices. The guidelines build on the original work from AEIC Guidelines v1.0-09-21-98, *Proposed AEIC Guidelines for Implementation of ANSI C12.19-1997 “Utility Industry End Device Data Tables,”* to define minimum requirements for ANSI C12.19-AMI interoperable End Devices, software, and firmware produced by AMI technology solutions providers that meet the requirements of NIST, AEIC and the SmartGrid interoperability.

2.2 Assumptions

It is critical to note that this document is a voluntary guideline for use by any Utility or other interested party for purchase order specifications of electronic metering devices and associated enterprise apparatus.

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.

This document is not intended to preclude other designs, manufacture, purchase, or use of any products not conforming to this document. This document is to be utilized when specifying an implementation of ANSI C12.19, “*Utility Industry End Device Data Tables*,” and required associated control service elements that are provided by Standard communication protocols that implement (E)PSEM. Users of these Guidelines need to evaluate their individual needs against those stated herein and decide on their applicability. This document is the framework and accreditation criteria to be used for ANSI C12.19 / IEEE 1377 / MC12.19 meters and other AMI devices by users and testers of this technology.

Familiarity of the user with ANSI C12.19-2008 is assumed in this document. For definitions and for the range of values possible, please reference C12.19-2008, ANSI C12.22-2008, ANSI C12.21-2006 and ANSI C12.18-2006, as appropriate.

2.3 Summary of Cybersecurity Content

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

The document references security phrases from the C12.18 and C12.21 documents, and comments on any issues.

Throughout the document, if the referenced security requirements need to be enhanced, a note similar to the following has been added “Note: ANSI C12.18 as presently written allows sending passwords in clear text on the communication path. This is a serious security issue. Passwords that are operational via optical port access using this protocol should not be operational when accessing the End Device via a Telephone/MODEM (such as ANSI C12.21) or over a network (e.g. ANSI C12.22).”

It does update or add very few additional requirements, such as “The security service is optional in those instances where the End Device does not implement the PSEM write service and all Tables are readable by any C12.18 client. Otherwise, the Security Service is required. When the Security Service is implemented by a C12.18 Device, the <password> element shall be compared with the PASSWORD elements of SECURITY_TBL (Table 42) of ANSI C12.19. When the passwords are not unique in the passwords Tables the highest authority (most permissive access) password that is operational via optical port shall prevail for this interface.”

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, *Guidelines to Smart Grid Cybersecurity*, Chapter 3, families and requirements, are shown in Table 1:

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

Reference in Standard ³	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.1.7 Communication Services	SG.AU-2 Auditable Events SG.AU-8 Time Stamps	
5.1.8 C12.19 Algorithms	SG.AU-8 Time Stamps	

³ The references may be just the section numbers or could include the title of the section

Reference in Standard ³	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
5.1.7.9 ANSI C12.22 Transport Layer Requirements	SG.SC-8 Communication Integrity SG.SC-9 Communication Confidentiality	
5.1.7.10 ANSI C12.22 Physical Layer Requirements	SG.PE-4 Monitoring Physical Access	
5.1.7.11 ANSI C12.22 Communication Module Requirements	SG.SC-8 Communication Integrity SG.SC-9 Communication Confidentiality SG.SC-12 Use of Validated Cryptography	
5.1.8 C12.19 Algorithms	SG.SC-12 Use of Validated Cryptography	
6.1.6 Meter and End Device Firmware Upgradability	SG.CM-5 Access Restrictions for Configuration Change	
6.2.1.5 Security Service	SG.SC-8 Communication Integrity SG.SC-9 Communication Confidentiality SG.IA-3 Authenticator Management	
6.3.1 Telephone MODEL Communications Using ANSI C12.21 / IEEE 1702 / MC 12.21		
6.4.1.2.5 APDU C12.22 Security / Authentication / Privacy	SG.IA-3 Authenticator Management SG.IA-5 Device Identification and Authentication SG.IA-6 Authenticator Feedback SG.SC-8 Communication Integrity SG.SC-9 Communication Confidentiality	
8.2.4 Event/Message Management & History Logs	SG.AU-2 Auditable Events SG.AU-3 Content of Audit Records SG.AU-8 Time Stamps	
8.2.8 Local Connectivity		
8.2.11 Meter Communications	SG.SC-12 Use of Validated Cryptography	

Reference in Standard ³	Applicable NISTIR 7628 Requirement	Comments if NISTIR Requirement Is Not Completely Met
8.2.21 Secure Communications	SG.SC-8 Communication Integrity SG.SC-9 Communication Confidentiality SG.SC-12 Use of Validated Cryptography	
8.2.24 Software / Firmware Upgrades	SG.AC-16 Wireless Access Restrictions	
8.2.25 Tamper Detection	SG.PE-4 Monitoring Physical Access	

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?

This document is about interoperability and it is necessarily to remember that incorporating security functionality should not impact the interoperability of a product.

Within various document sections, there is a note “ANSI C12.21 as presently written allows sending passwords in clear text on the communication path. This is a serious security issue. Passwords that are operational via telephone/MODEM access using this protocol should not be operational when accessing the End Device via a local port (such as ANSI C12.18 optical port, or ANSI C12.22 optical port) or over a network (e.g. ANSI C12.22).” This issue should be reviewed within the ANSI C12.21 standard.

The CSWG recommends the review of the ANSI C12 suite by a future PAP and/or DEWG to ensure cybersecurity requirements are adequately addressed.

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

No known activity at this time, although a new PAP or DEWG may be formed.

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

2.3.5.1 Normative References

- ANSI C12.18-2006: Protocol Specification for ANSI Type 2 Optical Port.
- ANSI C12.19-2008: Utility Industry End Device Data Tables.
- ANSI C12.21-2006: Protocol Specification For Telephone Modem Communication.
- ANSI C12.22-2008: Protocol Specification for Interfacing to Data Communication Networks.

- FIPS PUB 140-2: Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 25, 2001.
- Handbook for Electricity Metering, 10th Edition, Washington, District of Columbia, Edison Electric Institute, 2002, ISBN 0-931032-52-0.
- IEEE P1377-2010: Draft Standard for Utility Industry Metering Communication Protocol Application Layer (End Device Data Tables). Contains Errata for C12.19-2008.
- IEEE P1701-2009: Draft Standard for Optical Port Communication Protocol to Complement the Utility Industry End Device Data Tables. Same as C12.18-2006
- IEEE P1702-2009: Draft Standard for Telephone Modem Communication Protocol to Complement the Utility Industry End Device Data Tables, Same as C12.21-2006.
- IEEE P1703-2009: Draft Standard for Local Area Network/Wide Area Network (LAN/WAN) Node Communication Protocol to Complement the Utility Industry End Device Data Tables. Contains Errata for C12.22-2008.
- IETF RFC 768-1980: User Datagram Protocol, J. Postel.
- IETF RFC 791-1981: Internet Protocol, Information Sciences Institute University of Southern California.
- IETF RFC 793-1981: Transmission Control Protocol, J. Postel.
- IETF RFC 3376-2002: Internet Group Management Protocol, Version 3, B. Cain et. al.
- IETF RFC C1222 Transport Over IP - 2010: Draft ANSI C12.22, IEEE 1703 and MC12.22 Transport Over IP, A. Moise et. al.
- ISO/IEC 7498-1, 1994: Information Technology - Open Systems Interconnection - Basic Reference Model: The Basic Model.
- ISO/IEC 10035-1, 1995: Information Technology - Open Systems Interconnection - Connectionless Protocol for the Association Control Service Element - Protocol Specification.
- ISO/IEC 8825-1, 2002: Information Technology - ASN.1 Encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).
- ISO/IEC 62056-62, 2006: Electricity metering – Data exchange for meter reading, tariff and load control – Part 62: Interface classes (ANSI C12.19 Utility Tables class_id: 26).
- LUM-0610-01-V17: Recommendations for Establishing Electricity LUM Outside an Approved Meter – Final Report, 2009.
- NEMA SG-AMI 1-2009: Requirements for Smart Meter Upgradeability, 2009,
- Principles for Sealing Meters and Trade Devices, Measurement Canada, 1999-07-26.
- Specifications Relating to Event Loggers for Electricity Metering Devices and Systems (Measurement Canada, IS-E-01-E, 2003)
- XHTML 1.0 The Extensible HyperText Markup Language (Second Edition). W3C Recommendation 26 January 2000, revised 1 August 2002.
- XML Schema Part 1: Structures Second Edition, W3C Recommendation 28 October 2004