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

CSWG Standards Review Report

NIST Priority Action Plan 2

Guidelines for Assessing Wireless Standards for Smart Grid Applications

March 1, 2011

Security Assessment of Guidelines for Assessing Wireless Standards for Smart Grid Applications

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. 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 the typical cybersecurity requirements of these standards.

These caveats were taken into account as the information exchange standard(s) were reviewed.

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*).

[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.

- 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

As described in the Preface, "*This document represents an initial set of guidelines to assist Smart Grid designers and developers in their independent evaluation of candidate wireless technologies.*

This report is a draft of key tools and methods to assist Smart Grid system designers in making informed decisions about existing and emerging wireless technologies. An initial set of quantified requirements have been brought together for advanced metering infrastructure (AMI) and initial Distribution Automation (DA) communications. These two areas present technological challenges due to their scope and scale. These systems will span widely diverse geographic areas and operating environments and population densities ranging from urban to rural.

Applications requirements must be combined with as complete a set of management and security requirements for the life-cycle of the system. These requirements can then be used to assess the suitability of various wireless technologies to meet the requirements in the particular applications environment.

The wireless technologies presented here encompass different technologies that range in capabilities, cost, and ability to meet different requirements for advanced power systems applications."

The document is organized as follows:

- Section 1: Overview of the PAP 2 process
- Section 2: Acronyms and Definitions
- Section 3: Smart Grid business-level functional requirements, based on the Smart Grid conceptual model. This includes a discussion of Use Cases as the basis for implementation decisions, and identified the need for security management.
- Section 4: Characteristics of different wireless technologies, providing an overview of the Wireless Matrix spreadsheet. (The Wireless Matrix spreadsheet is included in this CSWG review).
- Section 5: Very detailed technical mathematical models of wireless technologies
- Section 6: Performance issues
- Section 7: Conclusions
- Sections 8 & 9: References and Bibliography.

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 assessing wireless communications within Smart Grid applications. This document is not intended to preclude other designs, manufacture, purchase, or use of any products not conforming to this document. This report investigates the strengths, weaknesses, capabilities, and constraints of existing and emerging standards-based physical media for wireless communications.

This report covers both business-level Use Cases (GWAC-stack Business Procedures layer) and the physical layer (GWAC-stack Basic Connectivity layer) of wireless technologies. Therefore, only security at those two layers should be addressed.

2.3 Assessment of Cybersecurity Content

The document recognizes that its treatment of cybersecurity is incomplete; Section 7, Conclusions, states, *"Going forward, this document may be revised as needed in order to include additional material contributed by PAP 2 members. Additional material may include examples on how to combine security and communication requirements and their implications on performance, additional communication requirements and wireless technology evaluation examples and models."*

.

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

Cybersecurity is addressed at a high level at the Business Procedures (Use Cases) layer through the SG Network TF Requirements Table which adds to each Use Case event the CIA (confidentiality, Integrity, and Availability) requirements as High, Medium, or Low.

Cybersecurity at the PHY/MAC layers are covered generically in this document, with references to the Wireless Matrix spreadsheet, Group 15, that lists the specific technologies used by different wireless technologies, including encryption, authentication, replay protection, key exchange, and rogue node detection. However, neither document assesses these security technologies in terms of their capabilities, vulnerabilities, performance impacts, applicability to networks or meshed networks, or other criteria.

Section 3.7 addresses the issue of cybersecurity by pointing to a database being developed by the OpenSG SG Communications SG Network Task Force. This database documents the Smart Grid business functional and volumetric requirements for input into the NIST PAP 2, but does not yet address cybersecurity.

Section 5.2 describes how models can be used to determine wireless characteristics. For instance, models of the PHY Layer in wireless technologies seek to minimize transmission failures due to noise, fading, etc. It also discusses the MAC Layer model performance handling for individual links, and the NET layer for handling end-to-end performance. These characteristics contribute to cybersecurity availability.

Although this document recognizes that cybersecurity should be addressed more fully, it does not do so yet.

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

The NISTIR 7628, *Guidelines to Smart Grid Cybersecurity*, is used as an informative reference within Version 1.0 of this guideline. 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
4.2.3 and Group 15 of the Wireless Matrix: encryption	SG.SC-12 Use of Validated Cryptography	The different wireless technologies use different types of cryptography – it is not clear if all are validated by NIST No assessments of the different security technologies are provided by these documents, making the claims unsubstantiated (but not necessarily untrue).
4.2.3 and Group 15 of the Wireless Matrix: authentication	SG.IA-5 Device Identification and Authentication	No assessments of the different security technologies are provided by these documents, making the claims unsubstantiated (but not necessarily untrue).
4.2.3 and Group 15 of the Wireless Matrix: replay protection	SG.SC-20 Message Authenticity	Protection against replay is only one aspect of ensuring message authenticity No assessments of the different security technologies are provided by these documents, making the claims unsubstantiated (but not necessarily untrue).
4.2.3 and Group 15 of the Wireless Matrix: key exchange	SG.SC-14 Transmission of Security Parameters	No assessments of the different security technologies are provided by these documents, making the claims unsubstantiated (but not necessarily untrue).
4.2.3 and Group 15 of the Wireless Matrix: rogue node detection	SG.IA-5 Device Identification and Authentication	No assessments of the different security technologies are provided by these documents, making the claims unsubstantiated (but not necessarily untrue).

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 document does not discuss how cybersecurity techniques are used or configured, nor does it address availability, key management, RF leakage, and wireless system vulnerabilities (as opposed to single wireless device vulnerabilities). These types of wireless system cybersecurity requirements also need to be addressed.

Section 3.7 states that security is only partially addressed in the Use Case database by the addition of CIA to Use Case events. It is not clear without reviewing that database to what degree cybersecurity is appropriately addressed that are relevant to wireless communications – many Use Cases may be entirely media-agnostic. However, some Use Cases should address cybersecurity issues that are directly related to the use of wireless media.

Several of the IEEE 802 standards include or are composed of provisions for cryptographic protection (such as encryption). None of these have been discussed, but they all should be.

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

There is no discussion regarding vulnerability of the modulation scheme to jamming or override (i.e., capture of the demodulator by a stronger signal). This needs to be considered.

Only the use of omni-directional antennas by the wireless technologies covered in the document was discussed. The use of directional antennas not only affects link power budget, but may also affect the ability of an intruder to intercept or jam communications. This security issue should be discussed.

It is technically feasible in setting the pseudo-noise (PN) sequences used for spread spectrum (whether direct sequence or frequency hopping) to use cryptographically derived PN sequences rather than published PN sequences, Using cryptographically derived PN sequences would force the intruder to first compromise the PN sequence to gain synchronism with the communications signal and then compromise the communication contents. Although the use of non-published PN sequences would be a policy issue, the technical possibility should be discussed and the policy issues posed.

Since this document does not assess the cybersecurity technologies for wireless systems, additional documentation is required to provide these assessments, not only for individual wireless equipment but also for different wireless configurations and performance requirements.

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?

There is a current task group working on an update to this guideline that will include members of the SG Network TF which will create a spreadsheet that relates the transactions between actors to the NISTIR 7628 logical interface categories and specifies the confidentiality, integrity, and availability of the data being transmitted and stored per transactions. This task group's output will show how the utility requirements for transactions can be mapped to the NISTIR 7628 high level security requirements..

2.3.5 Recommendations

The CSWG recommends the PAP-02 output document, Wireless Standards for the Smart Grid, be accepted as is, but that additional documents be developed in future efforts (in a DEWG or PAP) that:

- Address relevant key security requirements identified in the NISTIR 7628, *Guidelines for Smart Grid Cyber Security, and add normative references to* Volumes I-III. This effort would require completion of a risk assessment to determine applicable security requirements.
- Assess the various cybersecurity techniques used with wireless systems, as well as assess the impacts of these cybersecurity techniques on complete wireless systems, including the degree/type of security, performance considerations, configuration issues, and policies/procedures required to ensure their effectiveness.
- Develop additional Use Cases that cover wireless-specific cybersecurity requirements.

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

2.3.6.1 Normative References

- SG Network Systems Requirements Specification, v4.0, July 21, 2010. Available online at: http://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Latest_Release_Deliverables/

- Griffith, D., Souryal, M., Gentile, C., and Golmie, N., “An integrated PHY and MAC layer model for half-duplex IEEE 802.11 networks,” in Proc. IEEE Military Communications Conference (MILCOM), Nov. 2010.
- Bianchi, G., “Performance analysis of the IEEE 802.11 distributed coordination function,” IEEE J. Selected Areas Communications, vol. 18, no. 3, pp. 535–547, 2000.
- MAC protocols in wireless LANs,” Wireless Communications and Mobile Computing, vol. 4, no. 8, pp. 917–931, 2004.
- Gentile, C., Griffith, D., Souryal, M., and Golmie, N., “Throughput and Delay Analysis in Half-Duplex IEEE 802.11 Mesh Networks,” submitted to IEEE Intl. Conf. on Communications (ICC), Sept. 2010.
- Laselva, D., Zhao, X., Meinila, J., Jamsa, T., Nuutinen, J.-P., Kyosti, P., and Hentila, L., “Empirical Models and Parameters for Rural and Indoor Wideband Radio Channels at 2.45 and 5.25 GHz,” IEEE Intl. Symposium on Personal, Indoor, and Mobile Radio Communications, pp. 654-658, Sept. 2010.
- Xia, H.H., Bertoni, H.L., Maciel, L.R., Lindsay-Stewart, A., and Rowe, R., “Microcellular Propagation Characteristics for Personal Communications in Urban and Suburban Environments,” IEEE Trans. on Vehicular Technology, vol. 43, no. 3, Aug. 1994.
- Matolak, D.W., Remley, K.A., Gentile, C., Holloway, C.L., Wu, Q., and Zhang, Q. “Ground-Based Urban Channel Characteristics for Two Public Safety Frequency Bands,” Submitted to IEEE Trans. on Antennas and Propagation, Aug. 2010.
- Radio Frequency (RF) system scenarios, 3rd Generation Partnership Project, Technical Report 36.942, V8.2.0, June 2009.
- “SG-Network functional requirements spreadsheet, Version 3.0,” http://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Interium_Release_3/
- “SG Network System Requirements Specification Interim Release 3,” May 17, 2010, http://osgug.ucaiug.org/UtiliComm/Shared%20Documents/Interium_Release_3/
- “Working draft of Guidelines for using wireless communications,” http://collaborate.nist.gov/twikisggrid/pub/SmartGrid/PAP02Wireless/NIST_Priotity_Action_Plan_2_r04.pdf
- “cdma2000 Evaluation Methodology,” 3rd Generation Partnership Project 2, 3GPP2 C.R1002-B, http://www.3gpp2.org/Public_html/specs/C.R1002-B%20v1.0_Evaluation_Methodology.pdf
- “UHDR-DO Overview,” Qualcomm Incorporated contribution to 3GPP2 TSG-C Working Group 3, C30-20060626-031R1, ftp://ftp.3gpp2.org/TSGC/Working/2006/2006-06-MiyazakiJapan/TSG-C-2006-06-Miyazaki%20-%20Japan/WG3/C30-20060626-031R1_QCOM_UHDRDO_update.pdf
- “Results of L3NQS Simulation Study,” joint contribution from LG Electronics, Lucent Technologies, LSI Logic, Nortel Networks, Qualcomm Incorporated, and Samsung Electronics to 3GPP2 TSG-C Working Group 5, C50-20010820-011, August 20, 2001, ftp://ftp.3gpp2.org/TSGC/Working/2001/TSG-C_0108/TSG-C-0801-Portland/WG5/C50-20010820-011-Results%20of%20L3NQS%20Simulation%20Study.pdf
- “System Simulation Results for the L3NQS Framework Proposal for cdma2000 1x-EVDV,” joint contribution from LG Electronics, Lucent Technologies, LSI Logic, Nortel Networks, Qualcomm Incorporated, and Samsung Electronics to 3GPP2 TSG-C Working Group 5, C50-20010820-012, August 20, 2001, ftp://ftp.3gpp2.org/TSGC/Working/2001/TSG-C_0108/TSG-C-0801-Portland/WG5/C50-20010820-012%20L3NQS%20System%20Simulation%20Results.pdf
- "Summary of system-level simulation results presented by various companies for Rev-D development,” Qualcomm Incorporated contribution to 3GPP2 TSG-C Working Group 3, C30-20030812-062, August 12, 2003, ftp://ftp.3gpp2.org/TSGC/Working/2003/2003-08-Seoul/TSG-C-2003-08-Seoul/WG3/WG3%20Call,%202003.08.12/C30-20030812-062-Summary_system_simulation_results.doc

- IEEE 802.16m Evaluation Methodology Document, IEEE 802.16m-08/004r5 <http://ieee802.org/16/tgm/core.html#08_004> http://ieee802.org/16/tgm/docs/80216m-08_004r5.zip.
- Mobile WiMAX – Part I: A Technical Overview and Performance Evaluation, August 2006.

2.3.6.2 Informative References

- ISO/IEC27001 - International Organization for Standardization/International Electrotechnical Commission Standard 27001 –Information technology -- Security techniques -- Information security management systems -- Requirements
- NIST Special Publication 1108 - NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, January 2010
- NIST Internal Report 7628 - Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, August 2010
- NIST Internal Report 7628 -Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, August 2010
- NIST Internal Report 7628 -Guidelines for Smart Grid Cyber Security: Vol. 3, Supportive Analyses and References, August 2010