INL/EXT- 09-15658

U.S. Department of Energy
Office of Electricity Delivery
and Energy Reliability

Wireless Procurement Language in Support of Advanced Metering Infrastructure Security

August 2009

Reviewed By: ____________

Date: 9/18/09

NSTB

National SCADA Test Bed

Enhancing control systems security in the energy sector

DEPARTMENT OF ENERGY
UNITED STATES OF AMERICA

INL/EXT-09-15658

Wireless Procurement Language in Support of Advanced Metering Infrastructure Security

August 2009

Idaho National Laboratory
Idaho Falls, Idaho 83415

Prepared for the
U.S. Department of Energy
Office of Electricity Delivery and Energy Reliability
Under DOE Idaho Operations Office
Contract DE-AC07-05ID14517

DISCLAIMER

This information was prepared as an account of work sponsored by an agency of the U.S. Government. Neither the U.S. Government nor any agency thereof, nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness, of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. Government or any agency thereof.

EXECUTIVE SUMMARY

The Smart Grid applications that focus on the distribution areas of the power grid will be using the Advanced Metering Infrastructure (AMI) for data communications. The applications will be varied dependent on the utilities' implementation. Existing communication infrastructure will be used when possible, but in many cases, new communication infrastructure for residential meters will have to be installed. Most of these solutions will require a wireless application to the home residence or a wireless application inside the home for control and status of appliances. Meters located at home residences using wireless communications present a cyber security challenge. Cyber security requirements need to be requested at procurement to help manage this challenge.

This procurement language guidance for wireless communications was refined for the AMI Security Acceleration Project (ASAP) project, sponsored by the Department of Energy Office of Electricity Delivery and Energy Reliability (DOE-OE) National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB). The original wireless procurement language was developed for the Department of Homeland Security National Cyber Security Division Control Systems Security Program (DHS-NCSD-CSSP).

The information provided in the procurement language document does not forego the use of engineering practices. The system's prime requirements, functions, design, and expected behaviors need to be taken into account prior to adding or requesting security requirements.

INTRODUCTION

The U.S. Department of Energy (DOE) established the National Supervisory Control and Data Acquisition (SCADA) Test Bed (NSTB) to help industry and government improve the security of control systems used in the nation’s energy infrastructures. The NSTB is a multiple laboratory program and is funded and directed by the DOE Office of Electricity Delivery and Energy Reliability (DOE-OE). A key mission of the NSTB is to assess control systems and communication protocols for vulnerabilities that could put critical infrastructures at risk from a cyber attack. This task is in support of the Open Smart Grid subcommittee of the Utility Communications Architecture International Users Group (UCAIug), Advanced Metering Infrastructure Security (AMI-SEC) Task Force under the UtiliSec Working Group.[a]

An enabling component in the Smart Grid applications is the Advanced Metering Infrastructure (AMI) that will provide the data communications infrastructure for the power grid—mainly for distribution of power. Security requirements for AMI can be found in the AMI System Security Requirements V1.01 AMI Security Acceleration Project (ASAP) December 15, 2008 document.[b] This procurement language guidance for wireless communications focuses on procurement activities, whereas the AMI System Security Requirements may be used for procurement and overall security requirements in the design and implementation of AMI architecture. The following diagram shows some of the wireless communications expected in AMI architecture.

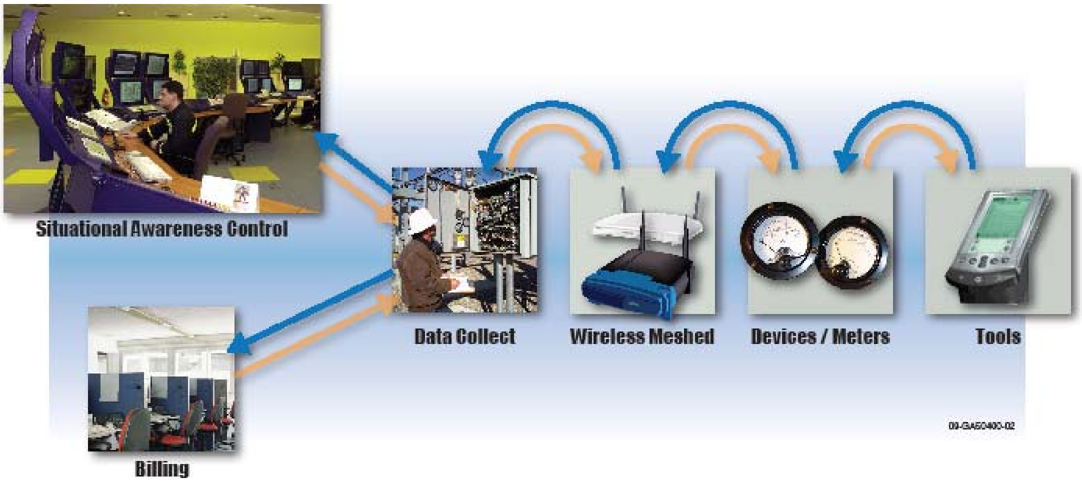

Figure 1. Overview AMI architecture for distribution communications.

Sections in this procurement specification include IEEE 802.11, WiMAX, Wireless Mesh, WirelessHART, Zigbee, Mobile Radio, Bluetooth, Cellular, and Microwave/Satellite. A matrix, with references to the existing procurement language, is provided for larger communications networks, end devices (meters), and perimeter protection architectures. Future topics that would be useful would include broadband over power line (BPL), power line carrier (PLC). The work was performed at Idaho National Laboratory (INL) from September 2008 until April 2009. The basis of this procurement specification is the Department of Homeland Security’s (DHS) Cyber Security Procurement Language for Control

[a] http://osgug.ucaiug.org/utilisec/amisec/default.aspx.

[b] http://www.marketwatch.com/news/story/collaborative-utility-task-force-partners/story.aspx?guid={54F1E24E-376C-4DA5-8ED5-1D60DE53F0C9}&dist=msr_5.

Systems.[c] The purpose of this document is to summarize security principles that should be considered when designing and procuring AMI wireless systems products and services (software, systems, maintenance, and networks), and provide example language to incorporate into procurement specifications. This guidance is offered as a resource for informative use; it is not intended as a policy or standard.

Figure 2 is a graph showing the range and data rate of common wireless technologies.

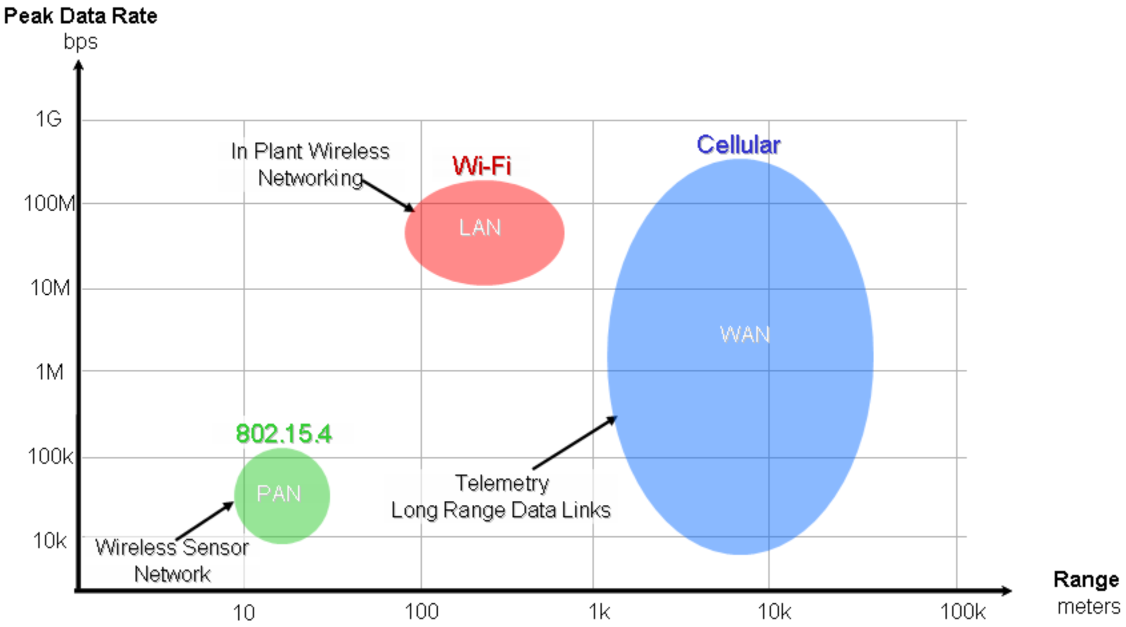

Figure 2. Overview of wireless technologies.

This document is designed to reduce cyber security risk in wireless communications by asking technology providers, through the procurement cycle, to assist in managing known vulnerabilities and weaknesses by delivering more secure systems. It initially targets high-value security risk reduction opportunities achieved through the procurement cycle.

This document includes a collection of security procurement language mapping directly to critical vulnerabilities observed in current and legacy wireless communications architectures that can be mitigated by technology providers and organizations through effective management of the technology across the systems' operational lifespan.

The information provided in the procurement language document does not forego the use of engineering practices. The system's prime requirements, functions, design, and expected behaviors need to be taken into account prior to adding or requesting security requirements.

The purchaser is encouraged to work with the vendor(s) to identify risk mitigation strategies specific to their system that may include solutions outside of those presented in this document. Many vendors are considered industry experts and are a valuable resource to the purchaser. It is not the intention of this document to discount the expertise leveraged by the purchaser.

[c] http://www.us-cert.gov/control_systems/pdf/SCADA_Procurement_DHS_Final_to_Issue_08-19-08.pdf.

TOPICAL TEMPLATE

This document is presented as a series of categorized high-level topics, each addressing a particular control system security area of concern. For each topic, the following information is provided:

Basis: A topic's basis is a summary of the potential exposures and vulnerabilities associated with a particular class of problem (i.e., why the topic is included).

Language Guidance: Additional information on the procurement language and how it intends to meet the needs described in the Basis.

Procurement Language: Example specification language is provided that can be included as part of procurement specifications to mitigate the Basis. References are made to specific timing of deliverable information. All language is agreed upon pre-contract award; proprietary or business sensitive information will be delivered after the contract is signed (post-contract award).

Note the terms "Factory Acceptance Test" and "Site Acceptance Test" are used generically; the testing cycles are described by regulatory agencies and are different for each sector.

Factory Acceptance Test Measures: The Factory Acceptance Test (FAT) is necessary to verify that security features function properly and provide the expected levels of functionality. Each topic includes FAT tasks specific to that topic. In general, prior to initiation of each FAT, the vendor shall install all operating systems and application patches, service packs, or other updates certified for use with the provided system by the time of test, and documentation of the configuration baseline. Note that FAT is a process, not an event, and could in fact extend over several weeks or months.

Site Acceptance Test Measures: The asset purchaser's Site Acceptance Test (SAT) typically repeats a subset of a FAT after system installation with additional integrated functions. Typically, the SAT is performed before the cutover or commissioning, to validate that the site installation is equivalent to the system tested at the factory. Like the FAT, the SAT may extend several weeks or months and may occur at multiple locations.

Maintenance Guidance: This is guidance on how the vendor will maintain the level of system security base lined during the SAT as the system evolves, is upgraded, and is patched. This subsection may be best included as a security clause in a maintenance contract, rather than in a procurement specification to maintain ongoing support.

References: External supporting information, practices, and standards are included.

Dependencies: Internal topics that should be in concert with the given topic.

CONTENTS

ACRONYMS

3G	Third Generation
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
APCO	Association of Public-Safety Communications
ASAP	AMI Security Acceleration Project
BERT	bit error test
BPL	broadband over power line
BSS	Basic Service Set
CB	Citizen Band
CDMA	Code Division Multiple Access
CSSP	Control System Security Program
DES	Data Encryption Standard
DHS	Department of Homeland Security
DoS	Denial-of-Service
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data Rates for GSM Evolution
EVDO	Evolution Data Only
FAT	Factory Acceptance Test
FRS	Family Radio Service
GMRS	General Mobile Radio Service
GPRS	General Packet Radio Service
GSM	Global System for Mobile Communications
HART	Highway Addressable Remote Transducer
HCI	Host Controller Interface
HTTP	Hypertext Transfer Protocol
IEEE	Institute for Electronics and Electrical Engineers
INL	Idaho National Laboratory
IP	Internet Protocol
ISA	International Standard for Automation
ISM	Industrial, Scientific and Medical
LAN	local area network
LMR	Land Mobile Radios

LoS	Line of Sight
LR	Low Rate
LR-WPAN	Low-Rate Wireless Personal Area Network
MAC	Medium Access Control
MPT	Mobile PMR Trunk
NCSD	National Cyber Security Division
NLoS	non-LoS
NSTB	National SCADA Test Bed
PHY	Physical Layer
PC	personal computer
PHY	physical
PKCS	Personal Key Encryption Algorithm
PKM	public key management
PMR	Professional Mobile Radio
RF	radio frequency
RSA	Rivest Shamir Adleman algorithm for public-key cryptography
SAT	Site Acceptance Test
SCADA	Supervisory Control and Data Acquisition
SHA-1	Secure Hashing Algorithm-1
SS	spread spectrum
SSH	Secured Shell
STA	Station
TETRA	Terrestrial Trunked Radio
TLS	Transport Layer Security
UCAlug	Utility Communications Architecture International Users Group
UHF	Ultra High Frequency
USB	Universal Serial Bus
VHF	Very High Frequency
WLAN	Wireless LAN
WEP	Wireless Enhanced Protection
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WMN	Wireless Mesh Network
WPA	WiFi Protected Access

Wireless Procurement Language in Support of Advanced Metering Infrastructure Security

1. 802.11 Technology

1.1 Basis

The reference, 802.11, refers to a family of specifications developed by Institute of Electrical and Electronics Engineers (IEEE) for wireless local area network (WLAN) technology. It specifies a wireless interface between a wireless device and a base station (access point) or between two wireless devices (peer-to-peer). 802.11 devices operate in the 5 GHz and 2.4 GHz public spectrum bands. Because these transmissions are through the air, these can be intercepted or interfered with by those having the proper equipment.

1.2 Language Guidance

There is only one current 802.11 standard. It is denoted by IEEE 802.11 followed by the date that it was published. The standard is updated by means of amendments. When a wireless device is referred to as 802.11*x*, *x* is an amendment to the original 802.11 standard. As of this date, IEEE 802.11-2007 is the most current 802.11 document available and contains cumulative changes (802.11a,b,d,e,g,h,i,j) from multiple sub-letter task groups. Care must be exercised when defining the 802.11 standard in procurement documents to be sure of the latest version.

The 802.11 standard, hereafter referred to as 802.11, defines the media access control (MAC) and physical (PHY) layers for a LAN with wireless connectivity where the connected devices are within close proximity to each other.

The Basic Service Set (BSS) is the basic component of an 802.11 wireless LAN. The BSS consists of a group of stations. The *station* (STA) is the basic component of the WLAN and is any device that provides the 802.11 protocol (MAC, PHY layers, and a connection to the wireless device). The station might be a personal computer (PC), handheld device, or an Access Point, and may be mobile or stationary.

Security is provided by encryption, authentication, and configuration control. The encryption methods used are Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), or WPA2. WEP can be easily intercepted and decoded. Numerous free software tools exist to aid in such endeavors. Due to these weaknesses, enhanced security was introduced for Wireless Fidelity (WiFi) networks through the WPA protocol. The security of connections using this protocol depends largely on the strength of the user-supplied pass-phrase. Free software and descriptions of how to attack these connections are also available online. Improving upon previous security implementations, the WiFi Alliance released the WPA2 standard, which uses a stronger encryption algorithm.

Despite the availability of strong encryption for user communication, the management frames of IEEE 802.11 messages are not encrypted, leaving the door open for Denial-of-Service (DoS) attacks. Several tools are available that can cause users to drop off the network or send messages to hamper the functionality of wireless end points. Such tools include WiFi jammers designed to block IEEE 802.11 transmissions, and rogue access points that are set up in hopes of attracting connections then stealing sensitive information or altering communications. Adding to and enabling attacks, is the fact that WiFi access points are often set up quickly and without security foresight. This results in the use of weak or no encryption, allowing attackers to impersonate wireless end points in hopes of providing false data. It also may result in users not changing default passwords for device management, allowing attackers to gain full control of the access point as default passwords are common knowledge. Recently, researchers have considered the possibility of worms that use the aforementioned security weaknesses to propagate on the local network. Such malicious code would rely on two assumptions to propagate. First, in urban settings, numerous WiFi networks exist within close proximity of one another. Second, that victim machines are configured to connect to multiple networks.

1.3 Procurement Language

The vendor shall provide the Wi-Fi device, meeting the requirements of the required sections of IEEE 802.11, and associated documentation.

Post-contract award, the vendor shall provide detailed information on communications (including protocols) required for the Wi-Fi device to communicate with the control network and the types of network devices with which the Wi-Fi device can communicate.

The vendor shall provide documentation on the range of the Wi-Fi device, power requirements, and the designated frequencies of operation for each device.

The vendor shall allow and recommend alarm settings in accordance to the needs of the system.

The vendor shall define interoperability limits for the Wi-Fi device specifically stating the devices that could be replaced and any associated problems that might be associated with the replacement.

The vendor shall provide, within a pre-negotiated period, any test data associated with the Wi-Fi device.

The Wi-Fi device shall be provided with security devices, such as passwords or security codes, to protect the device from unauthorized modification or use. The vendor shall clearly identify these security devices and methods to change these from the vendor-configured or manufacture default conditions.

The vendor shall provide the Wi-Fi device with the standard security measures as specified in the 802.11 standard and support the required level of encryption.

The vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the Factory Acceptance Test (FAT).

The vendor shall provide the purchaser Site Acceptance Test (SAT) procedures, which include exercising all functionality and calibration procedures.

The vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).

The vendor shall identify the configuration control options that enable varying of the security level of the device.

The vendor shall demonstrate that cooperative WiFi nodes can distinguish jamming from channel saturation and provide operational alerts.

The vendor shall provide test data showing that basic attacks, such as malformed packet injection, do not cause the WiFi device to crash, hang, or otherwise malfunction.

1.4 FAT Measures

The Factory Acceptance Test (FAT) shall be performed per written procedures agreed upon by the purchaser and in agreement with the requirements of the specified sections of 802.11.

For vendor-supplied Wi-Fi device, the vendor shall install the device and run it continuously during the entire FAT process.

The vendor shall ensure that the systems have had a minimum of a 48-hour burn-in.

The vendor shall perform an interference rejection test and supply the results with an explanation of the results.

The vendor shall ensure that FAT procedures include exercising all functionality, examining the input or output, and validating the results.

The vendor shall verify compatibility of the Wi-Fi device with other interfaced devices.

1.5 SAT Measures

The purchaser shall run the 802.11 system during the entire SAT process. SAT procedures shall include exercising this functionality, examining the log files, and validating the results.

Any vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time. The vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

The purchaser shall perform the SAT testing per the vendor-supplied procedures.

The SAT shall verify that the installed system meets the specified requirements.

The purchaser shall perform testing to analyze the potential for radio frequency (RF) interference, determine adequate wireless LAN coverage, and set configuration parameters properly.

1.6 Maintenance Guidance

The vendor shall supply current system configuration to the purchaser to allow traceability and to ensure no extra services are installed.

The vendor shall supply written maintenance guidelines for the device, including a timeline, maintenance equipment required, and as-left tolerances.

The vendor shall provide upgrades and patches to the Wi-Fi device as vulnerabilities are identified in order to maintain the identified level of system security.

1.7 References

Aime, M., G. Calandriello, A. Lioy, “Dependability in Wireless Networks,” IEEE Security and Privacy, January/February 2007.

Akriditis, P, et al, Proximity Breeds Danger: Emerging Threats in Metro-area Wireless Networks, 2007, http://www.usenix.org/events/sec07/tech/full_papers/akritidis/akritidis_html/metrowifi.html, Web page accessed March 2009.

Bellardo, J. and S. Savage, “802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions,” 2003, www.cs.ucsd.edu/~savage/papers/UsenixSec03.pdf, Web page accessed March 2009.

Gizmodo.com, Gadgets: Wireless Jammer, July 28, 2005, http://gizmodo.com/gadgets/gadgets/wireless-jammer-114698.php, Web page accessed March 2009.

IEEE 802.11, “The Working Group for WLAN Standards,” Institute of Electrical and Electronics Engineers, 2007.

IEEE Std 802.11i™-2004, “Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 6: Medium Access Control (MAC) Security Enhancements,” Institute of Electrical and Electronics Engineers, 2007.

Infrostream Technologies, Cellphone Jammers, WIFI/Bluetooth Jammers, Wireless Camera Hunter, http://www.infostream.biz/, Web page accessed March 2009.

J. Kirk, ‘Evil twin’ Wi-Fi access points proliferate, April 2007, http://www.networkworld.com/news/2007/042507-infosec-evil-twin-wi-fi-access.html, Web page accessed March 2009.

Phenoelit-us.org, Default Password List, http://www.phenoelit-us.org/dpl/dpl.html, Web page accessed April 2009.

T. Teska, “How To Crack WPA/WPA2,” January 2008, http://www.smallnetbuilder.com/content/view/30278/98/, Web page accessed March 2009.

Vladimirov, A., K. Gavrilenko, and A. Mikhailovsky, 2004, *WiFoo: The Secrets of Wireless Hacking*, Person/Addison Wesley, http://www.wi-foo.com, Web page accessed March 2009.

Wi-Fi Alliance, “WPA2 (Wi-Fi Protected Access 2),” 2007, http://www.wi-fi.org/knowledge_center/wpa2, Web page accessed March 2009.

1.8 Dependencies

None, this topic is stand-alone.

IEEE 802.15/Bluetooth, IEEE 802.11/WLAN, and IEEE 802.16/WiMAX technologies are complementary to each other and each play a unique role in today’s wireless communications.

2. WiMAX Technology

2.1 Basis

Worldwide Interoperability for Microwave Access (WiMAX) is a wireless broadband technology made for longer distances based on the IEEE 802.16 standard. WiMAX is a relatively new technology that can be configured for point-to-point links or mobile cellular type access. WiMAX uses both licensed and unlicensed frequencies: 2.3–2.7, 3.4–3.6, and 5.8 GHz bands. Like other wireless technologies, WiMAX security is dependent on vendor and owner/operator implementation. The optional nature of dual authentication techniques, per the standard, could allow for operation of a rogue station. Additionally, the lack of encryption of management frames could permit DoS attacks.

2.2 Language Guidance

While there are variations on the WiMAX standard, there are two versions of interest for industrial wireless systems: fixed WiMAX and mobile WiMAX. Fixed WiMAX is intended for point-to-point or multi-point links. This could be deployed in either the 5.8 GHz in the Industrial, Scientific and Medical (ISM) band, or other licensed frequencies. Point-to-Point WiMAX is very similar to how microwave is currently being used in industry today. Mobile WiMAX is being deployed in the commercial 2.5 GHz.

WiMAX security supports two quality encryptions standards: Data Encryption Standard (DES3) and Advanced Encryption Standard (AES). The standard defines a dedicated security processor on board the base station. There are also minimum encryption requirements for the traffic and for end-to-end authentication. For end-to-end authentication the public key management (PKM)-Extensible Authentication Protocol (EAP) methodology is used, which relies on the Transport Layer Security (TLS) standard of public key encryption. The key management protocol uses either EAP [IETF RFC 3748] or X.509 digital certificates [IETF RFC 3280] together with Rivest Shamir Adleman (RSA) public-key encryption algorithm (Personal Key Encryption Algorithm [PKCS] 1) or a sequence starting with RSA authentication and followed by EAP authentication.

2.3 Procurement Language

The vendor shall provide the WiMAX subscriber station equipment and associated documentation.

Post-contract award, the vendor shall provide detailed information on communications (including protocols) required for the WiMAX subscriber station to communicate with the base station and the types of network devices with which the wireless device can communicate.

The vendor shall provide documentation on the range of the WiMAX subscriber station, power requirements, and the designated frequency of operation for each device.

The vendor shall provide, within a pre-negotiated period, any test data associated with the WiMAX subscriber station to base station communications.

The vendor shall clearly identify these security devices and methods to change them from the vendor-configured or manufacture default conditions.

The vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.

The vendor shall provide the purchaser SAT procedures, which include exercising all functionality and calibration procedures.

The vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).

2.4 FAT Measures

The FAT shall be performed per written procedures agreed upon by the purchaser.

The vendor shall ensure that the systems have had a minimum of a 48-hour burn-in.

The vendor shall perform an interference rejection test and supply the results with an explanation of the results.

The vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results.

The vendor shall verify compatibility of the WiMAX equipment and communications with other devices with which the device must interface.

2.5 SAT Measures

The purchaser shall perform the SAT testing per vendor-supplied procedures.

The purchaser shall change any vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

The SAT shall verify that the installed system meets the specified requirements.

2.6 Maintenance Guidance

The vendor shall supply current system configuration to the purchaser to allow traceability and to ensure no extra services are installed.

The vendor shall supply written maintenance guidelines for the device, including a timeline, maintenance equipment required, and as-left tolerances.

The vendor shall provide upgrades and patches to the wireless device as vulnerabilities are identified in order to maintain the identified level of system security.

2.7 References

IEEE Standard 802.16e™, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Institute of Electrical and Electronics Engineers, pp. 269–313, 2005.

S. Petäjäsoja, et al., “Wireless Security: Past, Present and Future,” Codenomicon, February 2008, http://www.codenomicon.com/resources/whitepapers/Codenomicon_Wireless_WP_v1_0.pdf, Web page accessed March 2009.

WiMAX Forum™ Mobile System Profile, Release 1.0 Approved Specification, (Revision 1.4.0: 2007-05-02), 2007.

WiMAX Technology, “http://www.WiMAXforum.org/resources/frequently-asked-questions/, Web page accessed April 2009.

2.8 Dependencies

Section 1, “802.11 Technology”

3. Wireless Mesh Network Technology

3.1 Basis

A Wireless Mesh Network (WMN) is a communications network made up of radio nodes organized in a mesh topology. In WMNs, nodes are comprised of mesh routers and mesh clients. Each node operates not only as a host but also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations.

Potential vulnerabilities exist with the route management protocol, remote centralized management system, and over-the-air firmware upgrades via Internet Protocol (IP) Internet traffic, WMN operating system, and applications running on any node of the wireless mesh network such as SSH (Secure Shell) daemons or lightweight Hypertext Transfer Protocol (HTTP) servers. Because the transmissions between WMN nodes are through the air, these can be intercepted or interfered with by those having the proper equipment.

3.2 Language Guidance

Most, if not all IEEE 802.15.4-based technologies are WMNs. In addition to these networks, there are also other proprietary mesh network technologies. Regardless of technology, WMNs consist of the end devices or end nodes that could be a sensor or other asset. These assets are connected to the mesh network via a wireless router or repeater unit that is used to forward its data to the central host. Typically, these networks will have a special node called a gateway, which will connect the wireless network to the wire-line network. WMN integration with the Internet, cellular, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor networks, etc., can be accomplished through gateway and bridging functions in the mesh routers. Wireless Mesh Networks provide a method for the transport of data by routing the data through adjacent routers/nodes. This provides wide coverage by multiple smaller cells using wireless nodes to route data.

3.3 Procurement Language

The vendor shall provide the WMN, meeting the requirements of the required sections of IEEE 802.11, and associated documentation.

Post-contract award, the vendor shall provide detailed information on communications (including protocols) required for the WMN device to communicate with the control network and the types of network devices with which the WMN device can communicate.

The vendor shall provide documentation on the range of the WMN device, power requirements, and the designated frequencies of operation for each device.

The vendor shall allow and recommend alarm settings in accordance to the needs of the system.

The vendor shall define interoperability limits for the WMN device specifically stating the devices that could be replaced and any associated problems that might be associated with the replacement.

The vendor shall provide, within a pre-negotiated period, any test data associated with the WMN device.

Each WMN device shall be provided with security mechanisms, such as passwords or security codes, to protect the device from unauthorized modification or use. The vendor shall clearly identify these mechanisms and methods to change them from the vendor-configured or manufacture default conditions.

The vendor shall provide the WMN device with the standard security measures, as specified in the 802.11 standard, and support the required level of encryption.

The vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.

The vendor shall provide the purchaser SAT procedures, which include exercising all functionality and calibration procedures.

The vendor shall identify the configuration control options that enable varying of the security level of the device.

The vendor shall demonstrate that cooperative WMN nodes can distinguish jamming from channel saturation and provide operational alerts.

The vendor shall provide test data showing that basic attacks such as malformed packet injection do not cause the WMN device to crash, hang, or otherwise malfunction.

3.4 FAT Measures

The FAT shall be performed per written procedures agreed upon by the purchaser and in agreement with the requirements of the specified sections of 802.11.

For a vendor-supplied Wi-Fi device, the vendor shall install the device and run it continuously during the entire FAT process.

The vendor shall ensure that the systems have had a minimum of a 48-hour burn-in.

The vendor shall perform an interference rejection test and supply the results with an explanation of the results.

The vendor shall ensure that FAT procedures include exercising all functionality, examining the input or output, and validating the results.

The vendor shall verify compatibility of the Wi-Fi device with other interfaced devices.

3.5 SAT Measures

The purchaser shall run the 802.11 system during the entire SAT process. SAT procedures shall include exercising this functionality, examining the log files, and validating the results.

Any vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time. The vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

The purchaser shall perform the SAT testing per vendor-supplied procedures.

The SAT shall verify that the installed system meets the specified requirements.

The purchaser shall perform testing to analyze the potential for RF interference, determine adequate wireless WMN coverage, and set configuration parameters properly.

3.6 Maintenance Guidance

The vendor shall supply current system configuration to the purchaser to allow traceability and to ensure no extra services are installed.

The vendor shall supply written maintenance guidelines for the device, including a timeline, maintenance equipment required, and as-left tolerances.

The vendor shall provide upgrades and patches to the WMN device as vulnerabilities are identified in order to maintain the identified level of system security.

3.7 References

Akyildiz, I., X. Wang, W. Wang, "Wireless Mesh Networks: A Survey," Elsevier, 2004.

Bahr, M., "Proposed Routing for IEEE 802.11s WLAN Mesh Networks," WICON'06, The 2nd Annual International Wireless Internet Conference, Boston, Massachusetts, USA, August 2–5, 2006.

Edler, J., M. Oskowsky, W. Wang, "Wireless Mesh Network for Building Automation," Kiyon, http://wireless.industrial-networking.com/articles/articleprint.asp?id=1264, Web page accessed March 2009.

Mogre, P., M. Hollick, R. Steinmetz, "QoS in Wireless Mesh Networks: Challenges, Pitfalls, and Roadmap to its Realization," 17th International Workshop on Network and Operating Systems Support for Digital Audio & Video, Urbana-Champaign, Illinois, USA, June 4–5, 2007.

3.8 Dependencies

Section 1, "802.11 Technology"

Section 6, "ZigBee Technology"

Section 7, "Bluetooth Technology"

4. WirelessHART Technology

4.1 Basis

Wireless Highway Addressable Remote Transducer (HART) is a Wireless Mesh Network Communications Protocol designed to meet the needs of process automation applications. WirelessHART is a key part of the HART Field Communications Protocol Revision 7 and is backward compatible with existing HART devices and applications. The WirelessHART standard was approved in June 2007 and was released in September 2007.

WirelessHART is in the early stages of development and deployment; hence, there is not much publicly available information regarding its security. It shall be noted that because the IEEE 802.15.4 protocol is the basis for this technology, the previous IEEE 802.15.4 security analysis is applicable.

4.2 Language Guidance

The architecture of WirelessHART also supports field devices, gateways, and a network manager. There is a considerable similarity between this standard and the Zigbee standard. Since the creation of the

WirelessHART convergence committee in Industrial Standards Automation (ISA)100, WirelessHART will likely merge into ISA100.

WirelessHART uses IEEE 802.15.4-2006 compatible PHY and MAC Layer. Additionally, it supports hybrid Frequency Hopping SS and Direct Sequence SS. Securing communications is done with AES-128 block ciphers with individual Join and Session Keys and Data-Link Level Network Key. A primary objective of the WirelessHART standard is to be directly compatible with existing HART-enabled equipment, applications, and tools.

4.3 Procurement Language

The vendor shall provide, within a pre-negotiated period, any test data associated with the WirelessHART devices.

The WirelessHART device shall be provided with security devices, such as passwords or security codes, to protect the device from unauthorized modification or use. The vendor shall clearly identify these security devices and methods to change them from the vendor-configured or manufacture default conditions.

The vendor shall provide the WirelessHART device with the standard security measures as specified in the WirelessHART standard.

The vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.

The vendor shall provide the purchaser SAT procedures, which include exercising all functionality and calibration procedures.

The vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).

4.4 FAT Measures

The FAT shall be performed per written procedures agreed upon by the purchaser and in agreement with the requirements of the WirelessHART specification.

For vendor-supplied WirelessHART Network or vendor-provided WirelessHART Network configuration(s), the vendor shall install the WirelessHART Network or the configuration(s) and run the WirelessHART Network continuously during the entire FAT process.

The vendor shall ensure that FAT procedures include exercising this functionality, examining the log files, and validating the results.

The vendor shall ensure that the systems have had a minimum of a 48-hour burn-in.

The vendor shall perform an interference rejection test and supply the results with an explanation of the results.

The vendor shall verify compatibility of the WirelessHART device with other devices with which the device must interface.

4.5 SAT Measures

The purchaser shall run the WirelessHART Network during the entire SAT process. SAT procedures shall include exercising this functionality, examining the log files, and validating the results.

The purchaser shall change any vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

4.6 Maintenance Guidance

Changes may require an update to the WirelessHART Network configuration and/or documentation.

The vendor shall supply current system configuration to the purchaser to allow traceability and to ensure no extra services are installed.

The vendor shall supply written maintenance guidelines for the device, including a timeline, maintenance equipment required, and as-left tolerances.

The vendor shall provide upgrades and patches to the WirelessHART device as vulnerabilities are identified in order to maintain the identified level of system security.

4.7 References

Hale, G., "…WirelessHART products out and on the way," InTech Online Magazine, April 24, 2008, http://www.isa.org/InTechTemplate.cfm?Section=InTech_Home1&template=/ContentManagement/ContentDisplay.cfm&ContentID=68959, Web page accessed March 2009.

HART Communication Foundation, WirelessHART™ Technical Data Sheet, HCF_LIT-89, Revision 1.0B, May 15, 2007.

ISA100, Wireless Compliance Institute, http://www.isa.org/asci/ISA100-Wireless-Compliance-Institute-Prospectus.pdf Web page accessed April 2009.

4.8 Dependencies

Section 3, "Wireless Mesh Network Technology"

5. ZigBee Technology

5.1 Basis

ZigBee is a specification for a communication protocol using small, low-power digital radios based on IEEE 802.15.4 standard. It is more specifically known as Low-Rate Wireless Personal Area Networks (LR-WPAN) the name for a short-range, low-power, low-cost, low data-rate wireless multi-hop networking technology standard. Because these transmissions are through the air, these can be intercepted or interfered with by those having the proper equipment.

5.2 Language Guidance

The *ZigBee* Alliance is an association of companies involved with building specifications based on IEEE 802.15.4. This includes network, security, and application protocols. IEEE 802.15.4 specifies the physical layer and some of the data link layer. The higher layer protocols, in this case *ZigBee*, were developed by the *ZigBee* Alliance.

The *ZigBee* specification defines the higher-layer network and application services that build upon the IEEE 802.15.4 LR-WLAN standard. The networks can range from simple single-hop star topologies to more complex multi-hop mesh networks. *ZigBee* operates in the ISM radio bands.

ZigBee network features include self-organization, support for multi-hop routed networking topologies, interoperable application profiles, and security based on the AES.

5.3 Procurement Language

The vendor shall design and provide a configured *ZigBee* wireless network, meeting the requirements of the *ZigBee* specification, and associated documentation and running on a licensed frequency. The vendor shall configure the *ZigBee* network such that the following conditions are met:

1. The *ZigBee* network infrastructure shall be protected with a Network Key
2. Address filtering shall be employed at the MAC layer
3. The *ZigBee* encryption security service shall be utilized
4. Source node authentication shall be implemented
5. A personal area network (PAN) Identifier shall be pre-assigned and node connectivity shall be restricted
6. Out-of-band key loading method shall be used
7. Layer-2 security mechanisms supported in the IEEE 802.15.4 lower-layer MAC shall be enabled
8. Secure network admission control shall be implemented
9. Nodes with the Trust Center address shall be pre-configured.

The vendor shall provide detailed information on communications required for the LR-WPAN device to communicate with the control network and the types of network devices with which the LR-WPAN device can communicate.

The vendor shall provide documentation on the range of the LR-WPAN device, power requirements, and the designated frequency of operation for each device.

The vendor shall allow and recommend alarm settings in accordance to the needs of the system.

The vendor shall define interoperability limits for the LR-WPAN device specifically stating the devices the LR-WPAN device could replace and any associated problems that might be associated with the replacement.

The vendor shall provide, within a pre-negotiated period, any test data associated with the LR-WPAN device.

The LR-WPAN device shall be provided with security devices, such as passwords or security codes, to protect the device from unauthorized modification or use. The vendor shall clearly identify these security devices and methods to change them from the vendor-configured or manufacture default conditions.

The vendor shall provide the LR-WPAN device with the standard security measures as specified in the *ZigBee* standard.

The vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.

The vendor shall provide the purchaser SAT procedures, which include exercising all functionality and calibration procedures.

The vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).

The vendor shall identify the configuration control options that enable varying of the security level of the device.

5.4 FAT Measures

The FAT shall be performed per written procedures agreed upon by the purchaser and in agreement with the requirements of the *ZigBee* specification.

For vendor-supplied *ZigBee* Network or vendor provided *ZigBee* Network configuration(s), the vendor shall install the *ZigBee* Network or the configuration(s) and run the *ZigBee* Network continuously during the entire FAT process.

The vendor shall ensure that FAT procedures include exercising this functionality, examining the log files, and validating the results.

The vendor shall ensure that the systems have had a minimum of a 48-hour burn-in.

The vendor shall perform an interference rejection test and supply the results with an explanation of the results.

The vendor shall verify compatibility of the LR-WPAN device with other devices with which the device must interface.

5.5 SAT Measures

The purchaser shall run the *ZigBee* Network during the entire SAT process. SAT procedures shall include exercising this functionality, examining the log files, and validating the results.

The purchaser shall change any vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

5.6 Maintenance Guidance

Changes may require an update to the ZigBee Network configuration and/or documentation.

The vendor shall supply current system configuration to the purchaser to allow traceability and to ensure no extra services are installed.

The vendor shall supply written maintenance guidelines for the device, including a timeline, maintenance equipment required, and as-left tolerances.

The vendor shall provide upgrades and patches to the LR-WPAN device as vulnerabilities are identified in order to maintain the identified level of system security.

5.7 References

Daintree Networks, Inc., "Understanding 802.15.4 and ZigBee Networking," http://www.daintree.net/resources/index.php#primer, Web page accessed April 2009.

Gutierrez, J., E. Callaway, and R. Barrett, "Low-Rate Wireless Personal Area Networks: Enabling Wireless Sensors with IEEE 802.15.4™," IEEE Press, ISN 0-7381-3557-7, 2004.

IEEE 802.15.4-2003, http://grouper.ieee.org/groups/802/15/pub/TG4.html, Web page accessed March 2009.

IEEE 802.15-2006, http://grouper.ieee.org/groups/802/15/pub/TG4b.html, Web page accessed March 2009.

The ISA Working Group SP100 is developing standards for LR-WPAN industrial wireless technology and has created a set of application classes based on criticality/consequence for in-plant wireless systems ISA, http://www.isa.org/wsummit/presentations/SextonVancouverTalk.ppt, Web page accessed April 2009.

Werb, J., et al., "Improved Quality of Service in IEEE 802.15.4 Mesh Networks," Sensicast Systems and GE Global Research, http://www.cs.utexas.edu/~cdj/wia_files/submissions/008Final.pdf, Web page accessed March 2009.

ZigBee Alliance, http://www.ZigBee.org, Web page accessed March 2009.

5.8 Dependencies

Section 7, "Bluetooth Technology"

6. Bluetooth Technology

6.1 Basis

Bluetooth is designed as a cable replacement and personal area networking technology that allows freedom in placing devices without concern for running cables. Bluetooth broadcasts in the ISM band at 2.4 to 2.485 GHz, similar to other devices such as microwave ovens and cordless telephones. ISM is a license-free frequency band. Wireless technologies all have a common security risk in that anyone in the broadcasting area can intercept the transmission. Bluetooth-enabled devices have additional security risks, in that these provide a gateway to larger networks and other devices not using Bluetooth. Like other wireless technologies, security is provided using encryption, authentication, and configuration control.

6.2 Language Guidance

Bluetooth wireless technology is a short-range communications technology intended to replace the cables connecting portable and/or fixed devices and providing a method for connecting unrelated wireless and wired devices. The Bluetooth specification defines a uniform structure for a wide range of devices to connect and communicate with each other.

Bluetooth-enabled electronic devices connect and communicate wirelessly through short-range networks. It uses a frequency hopping spread spectrum technology to minimize the possibility of interference in the ISM band and encryption at the link or application levels to provide confidentiality and integrity for the transmitted data. Each device can simultaneously communicate with up to seven other devices within a single network. Line-of-sight (LoS) is not required. Most Bluetooth-enabled devices use omni-directional antennas for the communication, which eliminates orientation issues. Each device can belong to several networks simultaneously.

A complete Bluetooth application requires a Bluetooth controller (hardware device) that typically connects to a host computer through a Universal Serial Bus (USB) port, and additional services and higher-level protocols, known as the Bluetooth host, that are installed as software on the same host computer. Without proper configuration Bluetooth can allow any other Bluetooth device within radio proximity to access the system.

Security for a Bluetooth network is implemented through the frequency band hops, authentication, and encryption. The frequency hopping makes it difficult to eavesdrop. User authentication controls access to the network. The encryption provided is implemented using custom algorithms based on the SAFER+ block cipher and is secured at the 1, 40, and 64-bit levels.

6.3 Procurement Language

The vendor shall provide the Bluetooth-enabled device, meeting the Bluetooth specification, and associated documentation.

Post-contract award, the vendor shall provide detailed information on the communications (including protocols) required for the Bluetooth-enabled device to communicate with the control network and the types of network devices with which the wireless device can communicate.

The vendor shall provide documentation on the range of the Bluetooth-enabled device, power requirements, and the designated frequency of operation for each device.

The vendor shall define interoperability limits for the Bluetooth-enabled device, which specifically states the devices that the Bluetooth-enabled device could replace and any associated problems or additional hardware/software requirements that might be associated with the replacement.

The vendor shall provide, within a pre-negotiated period, any test data associated with the Bluetooth-enabled device.

The Bluetooth-enabled device shall be provided with security devices, such as passwords or security codes, to protect the device from unauthorized modification or use. The vendor shall clearly identify these security devices and methods to change them from the vendor-configured or manufacture default conditions.

The vendor shall identify the configuration control options that enable varying of the security level of the device.

The vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.

The vendor shall provide the purchaser SAT procedures, which include exercising all functionality and calibration procedures.

The quality of the implementation of the Bluetooth specification may vary from manufacturer to manufacturer (i.e., all Bluetooth implementations are not the same). The vendor shall provide test data showing that basic attacks such as malformed packet injection do not cause the receiving Bluetooth device to crash, hang, or otherwise malfunction.

6.4 FAT Measures

The FAT shall be performed per written procedures agreed upon by the purchaser.

For vendor-supplied Bluetooth-enabled device, the vendor shall install the device and run it continuously during the entire FAT process.

The vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results. The vendor will specify when the results are achieved at peak performance or are environment dependent.

The vendor shall ensure that FAT procedures include written validation and documentation of each requirement.

6.5 SAT Measures

The purchaser shall perform the SAT testing per vendor-supplied procedures.

The purchaser shall change any vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

6.6 Maintenance Guidance

The vendor shall supply current system configuration to the purchaser to allow traceability and to ensure no extra services are installed.

The vendor shall supply written maintenance guidelines for the device, including a timeline, maintenance equipment required, and as-left tolerances.

The vendor shall provide upgrades and patches to the Bluetooth-enabled device as vulnerabilities are identified in order to maintain the identified level of system security.

6.7 References

Bluetooth Special Interest Group, https://www.bluetooth.org/apps/content/, Web page accessed March 2009.

Bluetooth Specifications, http://www.bluetooth.com/Bluetooth/Technology/Building/Specifications/ Web accessed April 2009.

Gehrmann, C., J. Persson, B. Smeets, *Bluetooth Security*, Artech House, 2004.

Gratton, D., *Bluetooth Profiles*, Prentice Hall Publishers, 2003.

Palo Wireless, "Host Controller Interface (HCI)," http://www.palowireless.com/infotooth/tutorial/hci.asp, Web page accessed March 2009.

6.8 Dependencies

Section 6, "ZigBee Technology"

7. Mobile Radios

7.1 Basis

Mobile radios refer to wireless communications systems and devices that transmit and receive information, primarily voice, on radio frequencies. The transmitter and/or the receiver are mobile. Because these devices transmit wirelessly, these are subject to interception and modification of the signals.

7.2 Language Guidance

Mobile radios include walkie-talkies, Citizen Band (CB) radios, two-way radios, hand-held two-way radios, radio telephones, and mobile data transmittal devices. A modern mobile radio consists of a radio transceiver, housed in a single box, and a microphone with a push-to-talk release to listen button. A mobile radio must have an associated antenna. Other features of mobile radio systems may include point to multi-point communications, large coverage areas, closed user groups, and use of Very High Frequency (VHF) or Ultra High Frequency (UHF) bands.

Since these mobile radios are used primarily for voice communication, for this document mobile data transmittal devices or devices used to transmit sensitive voice communication are of primary concern. Those devices used for day-to-day voice communication are normally off-the-shelf and include no security devices, such as walkie-talkies and CB radios.

Different types of radio service for mobile radios include Land Mobile Radio (LMR) and General Mobile Radio Service (GMRS). LMR is a field radio communications system that uses portable, mobile, base station, and dispatch console radios typically used by police forces and fire brigades. LMR devices may be based on such standards as Mobile Professional Mobile Radio (PMR) Trunk (MPT)-1327, Terrestrial Trunked Radio (TETRA), and Association of Public-Safety Communications (APCO) 25. GMRS is a licensed land-mobile FM UHF radio service available for short-distance two-way communication, similar to Family Radio Service (FRS) radios. GMRS is an improved walkie-talkie system that shares some frequencies (Channels 1–7) with FRS. GMRS radios may be portable, mobile, and base station-style.

Mobile radio vendors are now offering IP-based mobile radio products. As mobile radios move into the IP-based digital domain, these products become susceptible to the same communications vulnerabilities as IP-based computer communications. This evolution, however, given the open network environment, introduces new security threats.

The following sections pertain only to those systems that transmit/receive sensitive information of control data. These shall not be used for the procurement or testing of off-the-shelf devices.

7.3 Procurement Language

The vendor shall provide the wireless mobile radio device and associated documentation.

Post-contract award, the vendor shall provide detailed information on communications (including protocols) required for the mobile radio to communicate with the control network and the types of network devices with which the wireless device can communicate.

The vendor shall provide documentation on the range of the mobile radio, power requirements, and the designated frequency of operation for each device.

The vendor shall provide, within a pre-negotiated period, any test data associated with the mobile radio.

The mobile radio shall be provided with security devices, such as passwords or security codes, to protect the device from unauthorized modification or use. The vendor shall clearly identify these security devices and methods to change them from the vendor-configured or manufacture default conditions.

The vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.

The vendor shall provide the purchaser SAT procedures, which include exercising all functionality and calibration procedures.

The vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).

7.4 FAT Measures

The FAT shall be performed per written procedures agreed upon by the purchaser.

The vendor shall ensure that the systems have had a minimum of a 48-hour burn-in.

The vendor shall perform an interference rejection test and supply the results with an explanation of the results.

The vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results.

The vendor shall verify compatibility of the mobile radio with other wireless devices with which the device must interface.

The vendor shall ensure that FAT procedures include written validation and documentation of this requirement.

7.5 SAT Measures

The purchaser shall perform the SAT testing per vendor-supplied procedures.

The purchaser shall change any vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

The SAT shall verify that the installed system meets the specified requirements.

7.6 Maintenance Guidance

The vendor shall supply current system configuration to the purchaser to allow traceability and to ensure no extra services are installed.

The vendor shall supply written maintenance guidelines for the device, including a timeline, maintenance equipment required, and as-left tolerances.

The vendor shall provide upgrades and patches to the wireless device as vulnerabilities are identified in order to maintain the identified level of system security.

7.7 References

GSM http://en.wikipedia.org/wiki/GSM Web accessed April 2009.

MPT 1327, A Signalling Standard for Trunked Private Land Mobile Radio Systems, http://wiki.radioreference.com/index.php/MPT-1327, Web page accessed March 2009.

Project 25, "APCO Project 25 and its Project 25 (P25) Standards for Public Safety Digital Radio," http://www.apco911.org/frequency/project25/information.html, Web page accessed March 2009.

TETRA RELEASE 1.3, ETSI 300 392-1 General Design http://portal.etsi.org/action/pu/20080603/tr_1003921704v010101p.pdf Web accessed April 2009.

7.8 Dependencies

None, this topic is stand-alone.

8. Cellular Technology

8.1 Basis

Monitoring and controlling equipment occurs at various points within an enterprise. In many cases, traditional cabled solutions or private radio networks are not a cost-effective option to cover all assets. Cellular technology may be used to manage and control industrial processes where cabling is not an option. Although the law provides penalties for the interception of cellular telephone calls, it is easily accomplished and impossible to detect.

8.2 Language Guidance

Cellular technology is being used in Supervisory Control and Data Acquisition (SCADA) environments when wide-area coverage is required and the cost of alternative technologies (Private Radio systems, Satellite, etc.) is uneconomical. Cellular is not available in some areas due to remoteness and lack of customer base.

Cellular modems are available that support both Code Division Multiple Access (CDMA) Evolution Data Only (EVDO) and Global System for Mobile Communications (GSM) protocols. Cellular routers may incorporate a cellular modem, or allow one to connect the cellular modem to the router, and support shared Internet access with multiple Ethernet ports. Packet data may be sent over cellular networks. The "always on" nature of packet networks makes these cellular packet data networks highly suitable for monitoring and control applications.

Cellular systems have had prolific growth in the last 10 years. Cellular systems have advanced three generations and standards are complete for fourth-generation technologies providing ultra high-speed wireless data. Standards primarily originate from two different technology families: CDMA and GSM. Despite the differences in the cellular families, both have very similar architectures.

Cellular technologies are categorized by using the term "generation" or G. Some earlier cellular technologies have had problems with security; however, 3G technologies have improved their security mechanisms significantly.

3G CDMA (EVDO) technologies include the use of 128-bit privacy and authentication keys. The Secure Hashing Algorithm-1 (SHA-1) is used for hashing and integrity with CDMA2000 networks (a hybrid 2.5G/3G network), while the AES algorithm is used for message encryption. GSM uses a similar encryption and authentication scheme known as the A5/A8 algorithm (a.k.a. A5/1, A5/2).

Some applications of cellular technology are as a cellular bridge or as a cellular gateway. A cellular bridge is a wireless bridge that uses a public cellular network to connect a remote device to a central host. These bridges use a cellular modem to provide connectivity. The cellular bridges can connect devices to an IP network by way of the Internet, or can use e-mail alarms or a short message service (SMS) to transmit and receive process control information. For instance, a BlackBerry device could be used to view process variables or control valves in a location that is remote from the user.

The cellular gateway is very similar to the cellular bridge. Cellular gateways use the cellular network to bring network information to a centralized control system or host, but also provide a separate wireless network, such as an access point, to support additional wireless devices. vendor offerings use General Packet Radio Service (GPRS), Enhanced Data Rates for GSM Evolution (EDGE) or EVDO for the cellular backhaul and WiFi for the Wireless LAN (WLAN).

The following sections pertain only to those systems that transmit/receive sensitive information of security or control data. This shall not be used for the procurement or testing of off-the-shelf devices for routine operations.

8.3 Procurement Language

The vendor shall provide the cellular system equipment and associated documentation.

Post-contract award, the vendor shall provide detailed information on communications (including protocols) required for the cellular system to communicate with the control network and the types of network devices with which the cellular system can interface.

The vendor shall provide documentation on the range of the cellular system, power requirements, and the designated frequency of operation for each device.

The vendor shall provide, within a pre-negotiated period, any test data associated with the cellular system.

The vendor shall provide the purchaser SAT procedures, which include exercising all functionality and calibration procedures.

The vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.).

8.4 FAT Measures

The FAT shall be performed per written procedures agreed upon by the purchaser.

The vendor shall ensure that the systems have had a minimum of a 48-hour burn-in.

The vendor shall perform an interference rejection test and supply the results with an explanation of the results.

The vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results.

The vendor shall verify compatibility of the cellular system with other devices with which the system must interface.

8.5 SAT Measures

The purchaser shall perform the SAT testing per vendor-supplied procedures.

The purchaser shall change any vendor-configured or manufacturer default usernames, passwords, or other security codes at this time. The vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

The SAT shall verify that the installed system meets the specified requirements.

8.6 Maintenance Guidance

The vendor shall supply current system configuration to the purchaser to allow traceability and to ensure no extra services are installed.

The vendor shall supply written maintenance guidelines for the device, including a timeline, maintenance equipment required, and as-left tolerances.

The vendor shall provide upgrades and patches to the wireless device as vulnerabilities are identified in order to maintain the identified level of system security.

8.7 References

IEEE 802.11n, "Standard for Enhancements for Higher Throughput," http://www.ieee802.org/11/Reports/tgn_update.htm Web accessed April 2009.

Mouly, M. and M. Pautet, "The GSM System for Mobile Communications," Cell and Sys Publishers, pp. 168–170, 1992.

NASA, "Cellular Phones," http://www.hq.nasa.gov/office/ospp/securityguide/V2comint/Cellular.htm, Web page accessed March 2009.

Pesonen, L., GSM Interception, November 1999, http://www.dia.unisa.it/professori/ads/corso-security/www/CORSO-9900/a5/Netsec/netsec.html, Web page accessed March 2009.

Wingert, C., M. Naidu, "CDMA 1xRTT Security Overview," Qualcomm, August 2002.

8.8 Dependencies

None, this topic is stand-alone.

9. Microwave and Satellite Technology

9.1 Basis

Both microwave and satellite communications use microwaves for transmitting information from point-to-point, both fixed and mobile. Point-to-point communication is directly between two points on the earth and requires unobstructed LoS. This is typical in a microwave communication link between two cellular network towers. Point-to-multipoint communication provides coverage from a single tower, which may include both LoS and non-LoS (NLoS) paths. Satellite communications transmit from a point on the earth to a satellite and then back to other points on the earth. Satellites introduce some potential latency, but can transmit over longer distances and provide connectivity in very remote areas. Microwave communications are preferable because satellite technology is the more expensive technology. Both microwave and satellite transmissions are susceptible to eavesdropping and intrusion techniques by those having the proper knowledge and equipment.

9.2 Language Guidance

Microwaves are electromagnetic waves in the radio frequencies between about 300 MHz and about 30 GHz with corresponding wavelengths of 1 m to 1 cm. Higher frequency waves have shorter wavelengths. Shorter wavelength transmissions have the advantage of being easier to control. These can be directed by small antennas, which helps keep the energy confined to a tight beam. This beam can be focused on another antenna many miles away. Since the beam is physically narrow, it is more difficult to intercept the signal. Another advantage to microwaves is that greater amounts of information (bandwidth) can be sent because of the high frequency.

LoS paths are limited in distance by the curvature of the earth, obstacles along the path, and free-space loss. These paths have a conservative range of 25 to 30 miles, but have been effective up to 100 miles. NLoS paths are generally used in the lower frequencies (<2 GHz) where refraction, diffraction, and reflection may extend communications coverage beyond LoS distances. The performance of both LoS and NLoS is affected by free-space path loss, terrain, atmosphere, and precipitation.

Microwave/satellite communication systems also use oscillators, amplifiers, and antennas as part of the communication system. The oscillator produces the transmission frequency; the amplifiers increase either the transmitted or the received signal, while the antenna, which is normally only 1 foot or a few feet across, provides the means to focus the signal.

Microwave links are very vulnerable to interception during transmission as the signal is sent across free-space line of sight links. Commercial equipment to tap into the signal for this kind of interception is readily and cheaply available. Fixed microwave facilities, such as office buildings, are common targets for this kind of interception as a very small rooftop antenna and decoder near the microwave link are all that is required. Antenna radiation patterns also present the opportunity for monitoring links outside direct LoS due to the presence of signal “sidelobes,” which can be picked up by sensitive receivers in the area. These systems can intercept microwave beams from satellites placed in appropriate positions.

9.3 Procurement Language

The vendor shall provide the microwave device, meeting the requirements of GR-63 NEBS™ and GR-1089, with associated documentation, and running on a licensed frequency.

Post-contract award, the vendor shall provide detailed information on communications (including protocols) required for the microwave device to communicate with the control network and the types of network devices with which the microwave device can communicate.

The vendor shall provide documentation on the range of the microwave device, power requirements, and the designated frequency of operation for each device.

The vendor shall allow and recommend alarm settings in accordance to the needs of the system.

The vendor shall define interoperability limits for the microwave device specifically stating the devices that could be replaced and any problems that might be associated with the replacement.

The vendor shall provide, within a pre-negotiated period, any test data associated with the microwave device.

The microwave device shall be provided with security features, such as passwords or security codes, to protect the device from unauthorized modification or use. The vendor shall clearly identify these security measures and the necessary methods to change them from the vendor-configured or manufacture default conditions.

The vendor shall remove or disable all software artifacts that are not required for the operation and maintenance of the device prior to the FAT.

The vendor shall provide the purchaser SAT procedures, which include exercising all functionality and calibration procedures.

The vendor shall document the equipment configuration and specifically note any security measures associated with the system (encryption devices, password protection, etc.). All information carried across the microwave links shall be secured through digital encryption.

9.4 FAT Measures

The FAT shall be performed per written procedures agreed upon by the purchaser and in agreement with the requirements of GR-63 NEBS™ and GR-1089.

For vendor-supplied microwave device, the vendor shall install the device and run it continuously during the entire FAT process.

The vendor shall ensure that the systems have had a minimum of a 48-hour radio/gear burn-in.

The vendor shall also apply a bit error test (BERT) for a minimum of 24 hours and verify that it has the agreed upon level of accuracy.

The vendor shall perform an interference rejection test and supply the results with an explanation of the results.

The vendor shall ensure that FAT procedures include exercising all functionality and examining the input or output, and validating the results.

The vendor shall ensure that FAT procedures include written validation and documentation of this requirement.

9.5 SAT Measures

The purchaser shall perform the SAT testing per vendor-supplied procedures.

Any vendor-configured or manufacturer default usernames, passwords, or other security codes must be changed at this time. The vendor shall ensure that SAT procedures include written validation and documentation of this requirement.

The SAT shall verify that the installed system meets the specified requirements.

9.6 Maintenance Guidance

The vendor shall supply current system configuration to the purchaser to allow traceability and to ensure no extra services are installed.

The vendor shall supply written maintenance guidelines for the device, including a timeline, maintenance equipment required, and as-left tolerances.

The vendor shall provide upgrades and patches to the microwave device as vulnerabilities are identified in order to maintain the identified level of system security.

9.7 References

GR-63-CORE, “NEBS™ Requirements: Physical Protection,” April 2002.

GR-1089-CORE, “Electromagnetic Compatibility and Electrical Safety - Generic Criteria for Network Telecommunications Equipment,” October 2002.

Senetas Security, “Whitepaper – Microwave Link Encryption,” June 2006.

9.8 Dependencies

None, this topic is stand-alone.

Appendix A

DHS: Cyber Security Procurement Language for Control Systems AMI-Sec Applicable Sections

Section	AMI-Sec Applicability	Comments
System Hardening	Data Concentrator Hosts	
Perimeter Protection	Overall Data Communications to Different Security Zones	
Account Management	Configuration Changes	The ability to change the configuration of a meter or reprogramming functions remotely should require advanced privileges.
Coding Practices	Meters and data communication applications	
Flaw Remediation	For maintenance of configuration	
Malware Detection and Protection	Data Concentrators and AMI-network	
Host Name Resolution	Addressing schemes	
End Devices	Meters are limited function end devices	The ability to remotely program meters are of special concern.
Remote Access	Common communications paths that may apply to communications to data concentrators	
Physical Security	Basic physical security requirements apply to meters and substations	Detect device tamper conditions and failure manual override capabilities
Network Partitioning	Applies to data traversing different security zones	