318

WI-FI PROTECTED ACCESS FOR PROTECTION AND AUTOMATION

Working Group
B5.22

April 2007

WI-FI PROTECTED ACCESS FOR PROTECTION AND AUTOMATION

Working Group B5.22

At the time this report was completed, Working Group 22 of CIGRE Study Committee B5 had the following membership [Corresponding Member is designated CM]:

Dennis HOLSTEIN (United States), *Convenor*

Jose Miguel ARZUAGA (Spain)
Todd DAVIS (United States)
Luc HOSSENLOPP (France - CM)
Russell HOUSLEY (United States - CM)
Tom KROPP (United States - CM)
Charles NEWTON (United States)
Mohindar SACHDEV (Canada)
Didier STOM (United States - CM)
Simon TERRY (United Kingdom)
Ivan SUSANTO (United States - CM)
Wai TSANG (United States - CM)
Darren WEBB (United Kingdom - CM)
David WHITEHEAD (United States)

n° ISBN : 978-2-85873-008-7

Table of contents

Table of figures

Table of tables

1. Introduction

If Wi-Fi[1], as defined by IEEE 802.11i, can be secured, the economic advantages for electric utility operations are significant. Wi-Fi is the industry standard for IEEE 802.11 compliant products and we know that Wired Equivalent Privacy (WEP) and Wireless Protected Access (WPA) systems are not secure. IEEE 802.11i defines how Wi-Fi systems work. It defines a new type of wireless network called a Robust Security Network (RSN) and Transitional Security Network (TSN) – RSN and WEP systems can operate in parallel. WPA and RSN share a common architecture and approach.

This technical brochure reports the findings and supporting data of work performed by CIGRE B5.22 by describing both the survey of applications using Wi-Fi in protection and automation schemes, and the mitigation of security vulnerabilities offered by IEEE 802.11i on system reliability and performance. Design requirements and security levels needed for Wi-Fi protected access are prioritized in terms of their mitigation of risk related to critical mission protection and automation functions. Specific mechanisms needed to adequately implement Wi-Fi are identified and relate to existing or emerging standards.

1.1 Scope

Study Committee B5 is responsible for studying principles, design, application and management of power system protection, substation control, automation, monitoring and recording. Working Group B5.22 was commissioned to survey applications using Wi-Fi in protection and automation schemes, and the mitigation of security vulnerabilities offered by IEEE 802.11i on system reliability and performance. B5.22 was also tasked to recommend design requirements and prioritized security levels needed for Wi-Fi protected access related to critical mission protection and automation functions.

Although there are many very good technical documents describing Wi-Fi available, B5.22 decided to use Reference [1] because of its clarity and excellent descriptive examples. Much of the text used in this technical brochure was extracted from Reference [1] and tailored for electric power transmission system applications. For the formal descriptions of cryptography, B5.22 used Reference [11]

Another good reference is NIST Special Publication 800-97 [17] that explain the security features and provides specific recommendations for federal US agencies to ensure the security of the operating environment. In particular, Chapter 8 in SP 800-97 describes the WLAN Security Best Practices, which are used to guide the supporting analysis for protection and automation in this technical brochure.

1.2 Purpose

This technical brochure discusses the impact of Wi-Fi protected access for substation protection and automation on the operation of equipment to reliably deliver electricity for distribution. Discussed are not individual functions of modern intelligent electronic devices (IEDs) but the overall aspects of how to use Wi-Fi to securely access the protection and automation functions. It applies for new substations as well as for refurbishment of secondary equipment in existing substations.

[1] Wi-Fi is promoted as the global brand name across all markets, and is not trademarked. Other terms that include Wi-Fi are trademarked; e.g., Wi-Fi Certified®.

The purpose is to assist engineers, who have not yet had experience using secure Wi-Fi applications to remotely manage equipment, by providing useful information gained by utilities, manufacturers, and system integrators.

Unless otherwise stated, the definitions provided in the IEEE 100 dictionary are used in this technical brochure [6] .

2. Summary of findings and recommendations

This report has considered the various experiences gained in many locations over a number of years in the use of Wi-Fi for protection and automation. It is recognized that because of known Wi-Fi vulnerabilities, availability, secure access, and confidentiality are the three primary concerns of the electric power operators. There have been a number of levels and complexities of such techniques and technologies employed to date and several new ones that are already being deployed.

This report cannot hope to define “the” right technology to use to meet a particular utility’s operational objective. However, it can serve as a guideline to utilities seeking to determine the range of solutions available and the issues that need to be considered in the final choice.

The following findings and recommendations are considered the most important. These deserve to be addressed in more depth by future CIGRE working groups.

1. Very few electric utilities are using Wi-Fi as defined by the IEEE 802.11i standard. Their primary concern is security. The survey covering 16 nations shows that Wi-Fi cost benefits are substantial and should be of great interest to the membership of all energy sector utilities (and industrial process control companies). Thus, there is an untapped market for solutions that provide real security in the near-time frame that can be cost justified by the asset owner.
2. ISO has accepted 802.11i, so we have an international security standard that provides the needed protection. What we don’t have is a recommended practice for applying the 802.11i standard to the energy sector.
3. The survey showed that 61% of those responding have not performed a risk assessment which includes Wi-Fi, nor do they plan to do so. This is very disturbing! Either the leadership doesn’t understand the problem or they don’t care. Clearly someone needs to take responsibility to raise the awareness of utility leadership to the potential threats and liabilities that could result by not taking prudent action.
4. Of the two approaches to key management, manual and automatic (electronic) systems, manual systems are more prone to risk. Manual systems significantly depend on human assistance, which has historically been the weakest component in any security architecture.
5. Radius servers can be used to generate “tags” to configure Virtual Local Area Networks (VLANs), which can be used to segregate user access to field devices. This means of access control provides more defense-in-depth against unauthorized access to these devices.
6. Antenna gain pattern shaping can be used to restrict the coverage area of a Wi-Fi access point within the substation fence so as to minimize access from outside the fence. Or, the pattern shaping can be used to restrict access to physically controlled or monitored areas outside the substation fence.

7. Most Wi-Fi equipment found at commercial retail stores does not meet the environmental requirements for operation in a substation. The Wi-Fi equipment must not induce undesirable operations; such as those equivalent to “no false trips” in relaying parlance.

3. What was learned from the Wi-Fi use survey

The research study on the use of Wi-Fi wireless communications in electric power substations was undertaken by the Newton-Evans Research Company on behalf of CIGRE B5, Working Group 22 during January to May 2006. The survey was sent to approximately 400 leading electric power utilities, each serving at least 50,000 customers, and most serving more than one million customers, and having at least 20 electric power distribution and/or transmission substations around the world.

By May 8, 2006, officials from 83 utilities from 32 countries participated in the research program. Appendix G is a list of the participating countries.

Across the world, there was little difference in current practices regarding the use of Wi-Fi wireless technology adoption and use. That is to say, utility officials were not likely to be using Wi-Fi or wireless technology of any type by mid-2006 for sensitive mission-critical applications, such as protection and automation.

The results of the Wi-Fi survey are reinforced by another study conducted by the Newton-Evans Research Company – see Reference [19] . The results of this study and its influence on the findings for the Wi-Fi study are summarized in Appendix H.

3.1 Communications inside the substation fence

The survey showed that 84% (Figure 1) of those responding do not currently use WLAN inside the substation fence. Most were already using some form of “wired” approach (fiber, copper, cable).

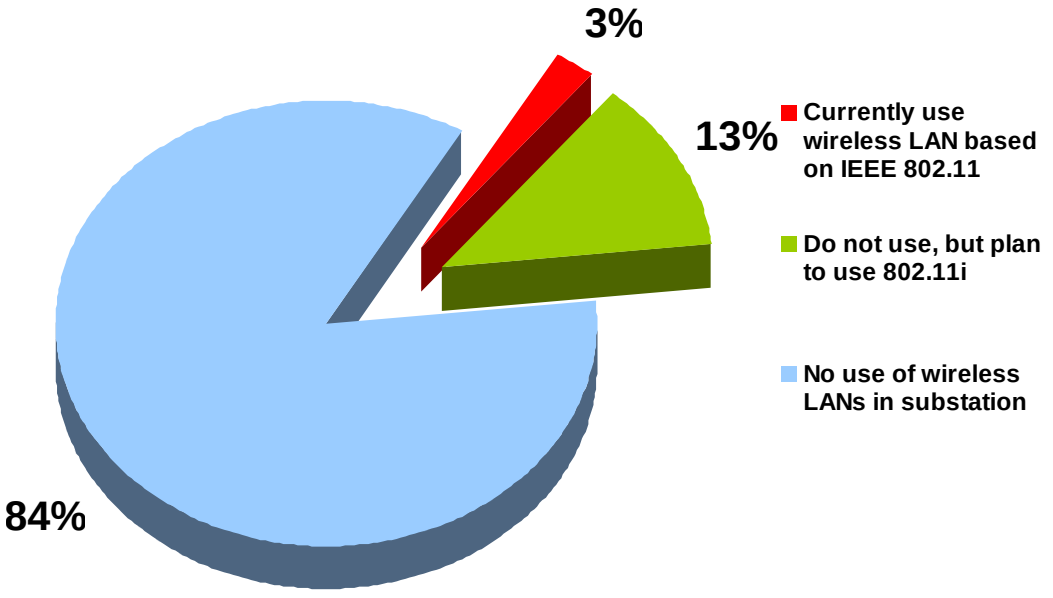

Figure 1 Little current use of Wi-Fi inside the substation fence

3% currently use WLAN and 13% do not use WLAN, but will use 802.11i. This response is highly correlated with the security issue, which shows 71% do not use WLAN because it lacks sufficient security. This is reflected in the company's standing security policy and based on articles discussing the security risks. Still other officials indicated that their reluctance to use WLAN in substations was based more on recent upgrades to wire line communications rather than security concerns.

Now that ISO has accepted 802.11i, a security standard is in place that provides the necessary protection. What is not available is a recommended practice for applying the 802.11i standard to the energy sector. This technical brochure provides much of the technical data needed by any standards-making organization to develop the recommended practice or standard.

3.2 Wi-Fi to access IEDs at any time regardless of location

The survey response to the benefit of having the capability to use Wi-Fi to access IEDs at any time regardless of location are most encouraging. Figure 2 shows that 3% already use this capability and an additional 11% will join this club in the next two years. However, the best news is that an addition 66% could use the benefit offered by Wi-Fi, but have not made plans to do so at this time. CIGRE and the vendor community offering Wi-Fi solutions for this application have an excellent opportunity to educate and market this capability. Clearly, the cost benefit is substantial and should provide an excellent market entry opportunity.

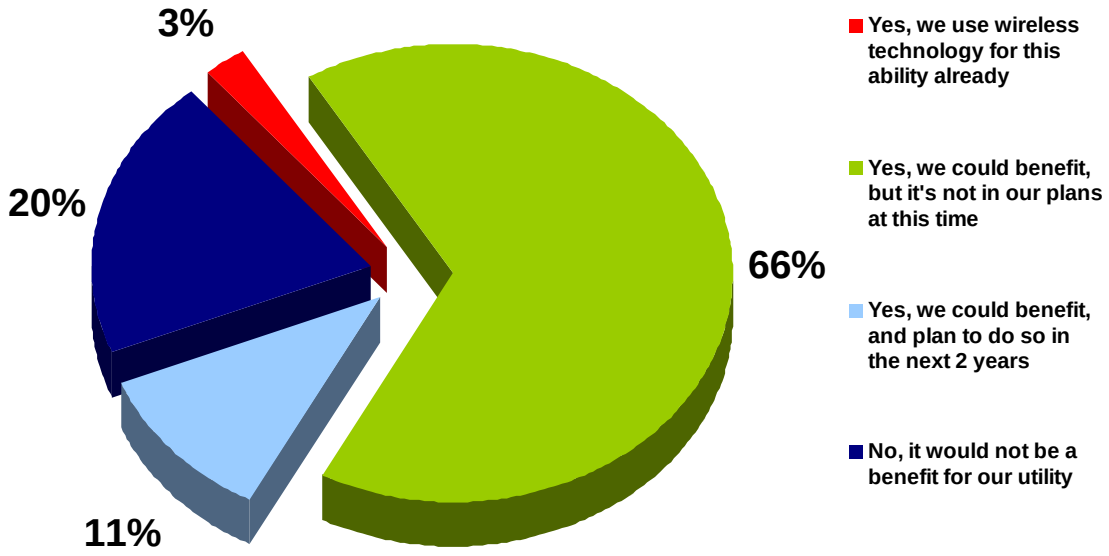

Figure 2 Utility executives recognize the benefit of using a secure WLAN

Another option is to restrict this use to local access without entering the substation fence. Again, Figure 3 shows that 3% use Wi-Fi for this already – probably the same 3%

discussed above. More encouraging is that an additional 17% will join this club in the next two years. This is up from 6% discussed earlier. Again, a large population of 36% could benefit, but have not made plans to do so. It seems that this market entry has a more near term pay-off because it offers a significant security advantage. Using Wi-Fi, the field technicians could access substation IEDs without requiring physical access to the substation.

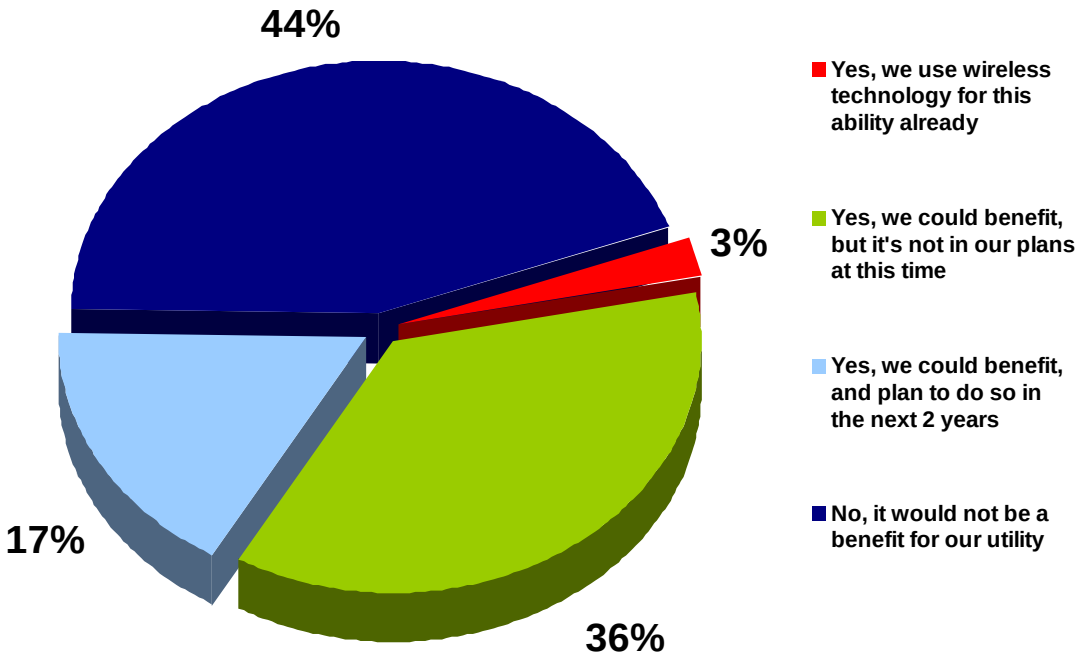

Figure 3 Utility executives like the idea of being able to access substation IEDs with entry into the substation

Another subset of local access addressed the question of using Wi-Fi to access IEDs that are difficult to reach because of terrain or environmental conditions. Figure 4 shows that 1% use Wi-Fi for this purpose and additional 13% plan to do so in the next two years. 24% see the benefit, but have not made plans to do so.

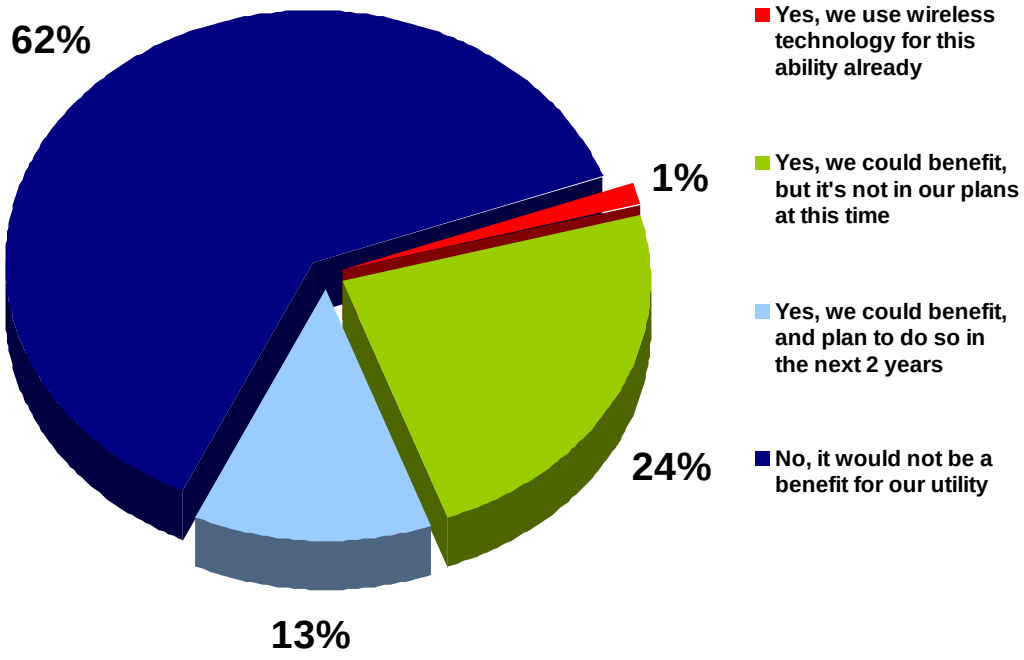

Figure 4 Hard to reach IEDs could use Wi-Fi

Probably within the statistical significance of the survey, Figure 3 and Figure 4 tell the same story. Secure Wi-Fi is a cost effective solution to access IEDs without entering the substation or accessing IEDs that are in hard-to-reach locations. The market opportunity is obvious, but some education is needed to show the utility engineers that the solution is secure.

3.3 The issue is security

One of the surprising responses received was the answer to the question “Has a security risk assessment been performed at your utility that includes possible use of wireless communications for protection and automation.” Figure 5 shows that 61% said they had no plans for such a security risk assessment which includes Wi-Fi – given the world-wide emphasis on cyber security by each national government, this is surprisingly high. Those 61% don’t understand the problem; or no matter what the benefit, they have no plan to use Wi-Fi for protection and automation under any circumstances – therefore, they don’t need to perform a risk assessment.

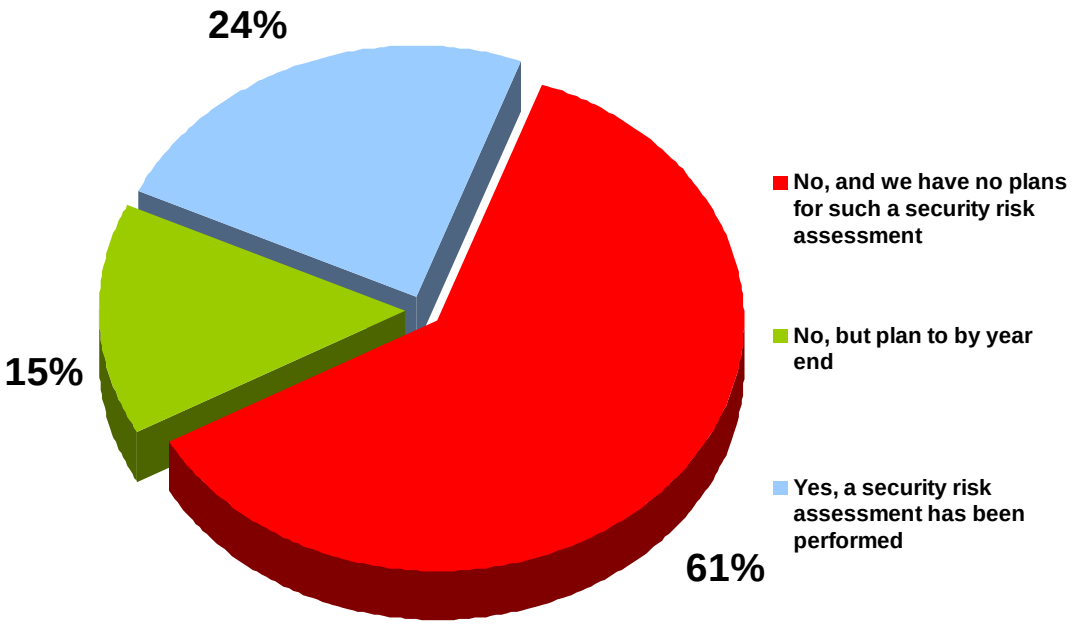

Figure 5 Surprising news regarding risk assessment

The good news is that 24% have performed a security risk assessment, and an addition 15% plan to do so by the end of 2006.

Future discussion with utilities should begin with this question. Their answer will then lead to significantly different lines of discussion.

3.3.1 The issue of using Wi-Fi for mission critical tasks

As illustrated in Figure 6, the survey showed almost an equal split on whether or not security is a concern for monitoring – remote capturing metering data; 35 officials (45%) were not concerned and 42 (55%) were concerned.

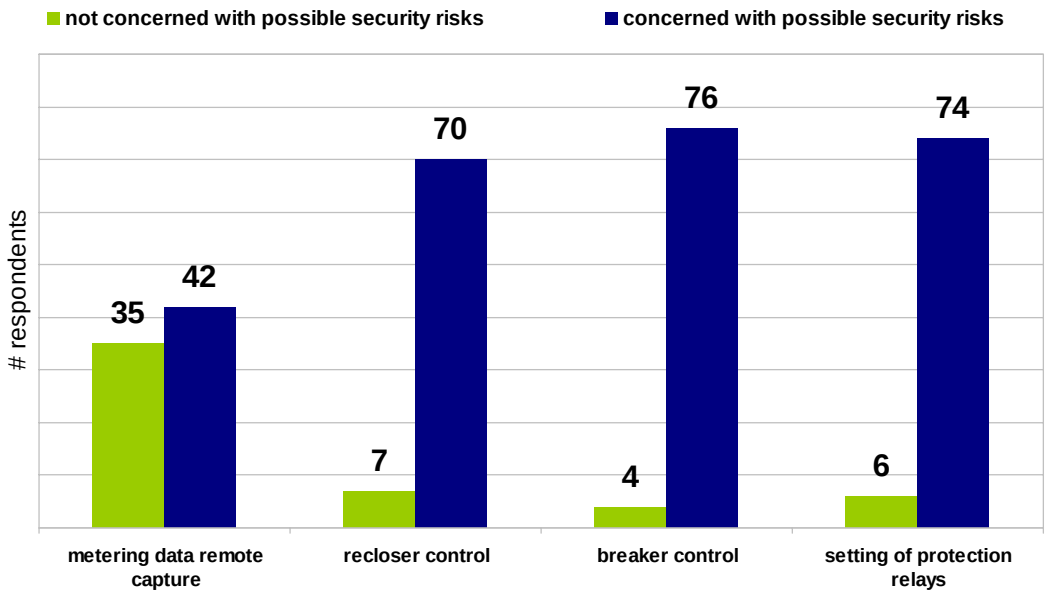

Figure 6 Wi-Fi for control and protection is a tough sell

The story is quite different for control and protection functions involving recloser control, breaker control or setting protection relays. In all cases 70 to 74 officials (or more than 90% of those responding) had security concerns about use of WLAN for mission critical tasks, and 4 to 7 (fewer than 10%) were not concerned.

Clearly the easier market entry point is to use Wi-Fi for monitoring. Control and protection is going to be a tough sell for WLAN.

3.3.2 A similar story for operational applications

Of those responding, Figure 7 shows that 23 respondents plan to use Wi-Fi for control of energy management, 52 do not. Control of SCADA is similar: 30 respondents plan to use Wi-Fi, and 47 do not. Only 15 respondents plan to use Wi-Fi for management and control of generation, 57 do not. And, only 18 respondents plan to use Wi-Fi for management and control within substations, 60 do not.

It should be noted that various radio communication methods, including microwave are not considered “wireless” technologies for the purpose of this survey.

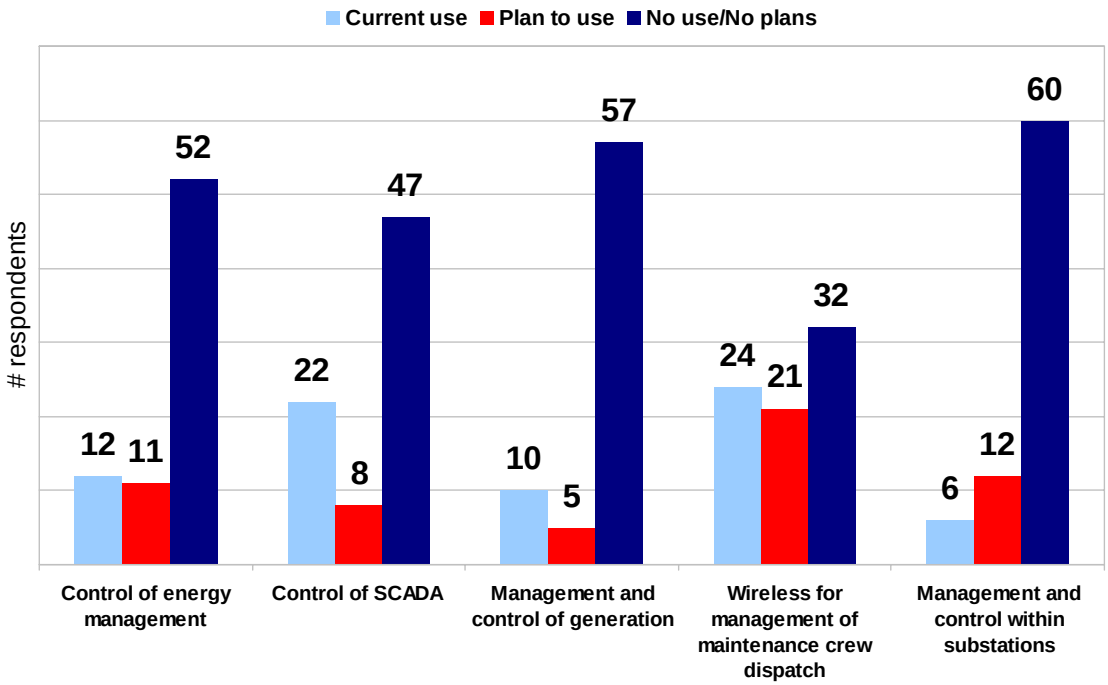

Figure 7 Mixed messages for other operational applications

However, the story for management of maintenance crew dispatch is more encouraging. 45 respondents plan to use Wi-Fi and 32 do not.

The natural market entry point is for management of maintenance crew dispatch. As this application of WLAN becomes more widely implemented, the use of Wi-Fi may well become more attractive to the other operational applications.

3.3.3 The Wi-Fi market looks good for enterprise applications

Figure 8 shows that Wi-Fi is definitely attractive for other applications. Of those responding, 55 officials (75%) plan to use Wi-Fi for voice applications, 18 (25%) do not. 40 respondents (57%) plan to use Wi-Fi for paging, 30 (43%) do not. 35 respondents (49%) plan to use Wi-Fi for asset management, 37 (51%) do not. And 30 respondents (43%) plan to use Wi-Fi for inventory management, 40 (57%) do not.

Although somewhat balanced between the will do and will not, the market entry for use of Wi-Fi for those applications look promising.

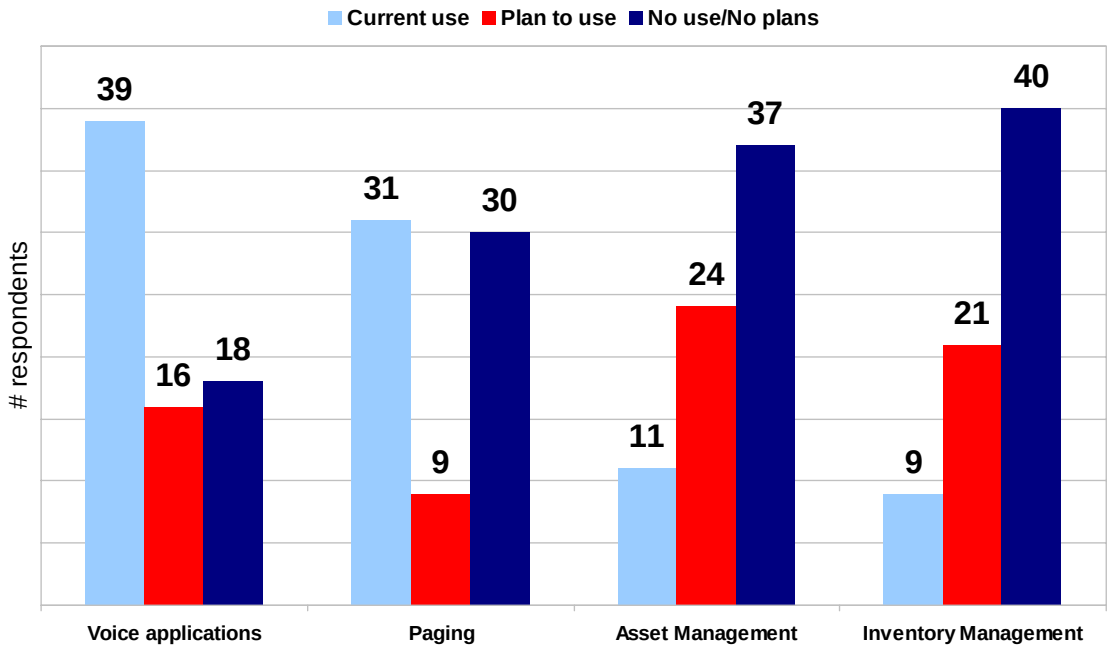

Figure 8 Wi-Fi is definitely attractive for other applications

4. An architectural view on the use of Wi-Fi for protection and automation

Figure 9 shows a very simplified view of Wi-Fi access to substation RTUs and IEDs. This view mirrors the questions asked in the survey and forms the basis for the remaining technical discussion of this brochure. Specifically, access to SCADA data from outside the substation fence and access to the maintenance ports of an IED or RTU from outside the substation fence are of particular interest.

Figure 9 also includes the common dial-up access to the maintenance ports of field devices. The technician's laptop computer may be configured to provide both dial-up and Wi-Fi access so that either can be used.

Access to SCADA data is possible, but as the survey showed, this is not common practice. It is included in the basic architecture diagram because as Wi-Fi becomes more common place, this function may also be of value to the utility.

Defense-in-Depth (DiD) is extremely important to restrict access to field devices to only those who are authorized. Chapter 6 focuses attention on the strategy needed to implement an effective Defense-in-Depth. DiD is further enhanced by using "tags" to configure VLANs to segregate users – see Section 4.5, and Wi-Fi antenna gain pattern shaping to restrict coverage areas – see Appendix F.

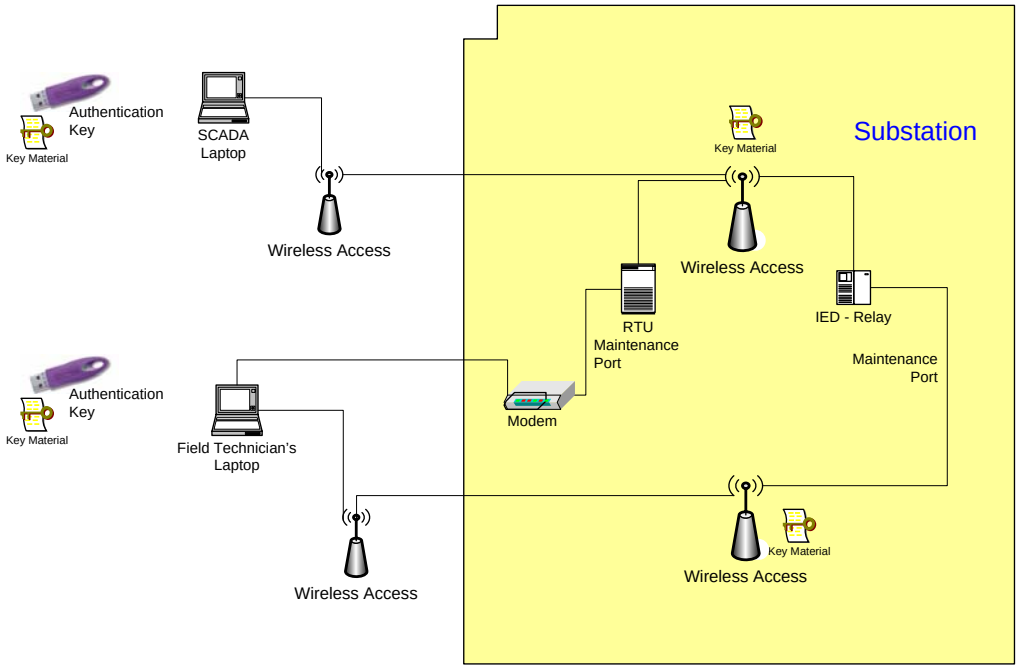

Figure 9 Very simplified view of Wi-Fi access to substation RTU/IED

4.1 Selected uses for the radio spectrum

Table 1 shows the selected uses for the radio spectrum, and highlights the two frequency bands allocated for Wi-Fi. These free/unlicensed bands are normally referred to as Industrial, Scientific, Medical (ISM) radio bands that were originally and internationally reserved for non-commercial use. In recent years they have also been used for licensed-free error-tolerant communication applications.

Table 1 Selected uses for the radio spectrum

AM radio	535 kHz – 1.7 MHz
Baby monitor	49 MHz
FM radio	88 -108 MHz
Wildlife tracking collars	215 – 220 MHz
Cell phones	824 – 849 MHz
Free/unlicensed - ISM (Wi-FI)	2.39 – 2.415 GHz
Aeronautical navigation	5 – 5.25 GHz
Free/unlicensed – ISM (Wi-Fi)	5.47 – 5.95 GHz
Satellite (fixed)	5.925 – 7 GHz

4.2 Comparative speeds of 802.11 implementations

Table 2 shows the comparative speeds of 802.11 implementations including comparison with Bluetooth and 10basedT implementations. Actual measured estimates of 802.11b are 6 Mbps versus the theoretical speed of 11 Mbps.

Table 2 Comparative speeds of 802.11 implementations

Bluetooth	.38 Mbps	
802.11b	6 Mbps	Actual estimate
10basedT (wired)	10 Mbps	
802.11b	11 Mbps	Theoretical
802.11a	24 Mbps	Theoretical
802.11g	54 Mbps	Theoretical
802.11i	54 Mbps	Theoretical based on 802.11g
802.11n	200+ Mbps	Theoretical

Protection and automation throughput performance requirements specified in several international standards can operate over high speed 802.11 implementations – See References [12] [13] [14] IEEE 802.11b is probably marginal for some high speed requirements, but 802.11g and 802.11n are very attractive because they offer wireless connections with adequate speed for almost all applications.

A better understanding of throughput performance is to compare their Over-the-Air (OTA) estimates and Media Access Control (MAC) Layer Service Access Point (SAP). Estimates for each IEEE WLAN standard are shown in Table 3 (Source: Intel Labs [15]). To be conservative, the substation communication design engineer should use the lower MAC SAP estimate as a basis for analysis.

Table 3 Throughput by IEEE Standard

IEEE WLAN Standard	**OTA Estimate**	**MAC SAP Estimate**
802.11b	11 Mbps	5 Mbps
802.11a	54 Mbps	25 Mbps
802.11g	54 Mbps	25 Mbps (when .11b is not present
802.11n	200+ Mbps	100 Mbps

Three key areas were addressed to achieve the increase in wireless LAN performance.

- Improvements in radio technology to increase the physical transfer rate.
- New mechanisms implementing the effective management of enhanced Physical Layer (PHY) performance modes.
- Improvements in data transfer efficiency to reduce performance impacts of PHY headers and radio turnaround delays that would otherwise reduce the improvements achieved with increases in physical transfer rate.

4.3 Increasing the physical transfer rate may increase cost

One approach to increasing the physical transfer rate employs multiple antenna systems for both the transmitter and receiver. This technology is referred to as multiple-input multiple-output (MIMO), or smart antenna systems. MIMO exploits the use of multiple signals transmitted into the wireless medium and multiple signals received from the wireless medium to improve wireless performance. Two benefits offered by MIMO

should be considered by the substation communication design engineer. However, keep in mind that this increasing complexity translates to higher implementation cost to gain the increased throughput performance.

4.3.1 Antenna diversity

Using multiple antennas, MIMO provides the ability to coherently resolve information from multiple signal paths using spatially separated receive antennas. Multipath signals are the reflected signals arriving at the receiver some time after the original or line of sight (LOS) signal has been received. Multipath is typically perceived as interference degrading a receiver's ability to recover the intelligent information. Because MIMO can spatially resolve multipath signals, this diversity gain contributes to the receiver's ability to recover the intelligent information.

4.3.2 Spatial division multiplexing

Spatial Division Multiplexing (SDM) spatially multiplexes multiple independent data streams, transferred simultaneously within one spectral channel of the bandwidth. MIMO SDM can significantly increase data throughput as the number of resolved spatial data streams is increased. Each spatial stream requires its own transmit/receive antenna pair at each end of the transmission.

4.4 Legacy coexistence

The IEEE Task Group "n" requires backward compatibility with 802.11a/b/g devices. 802.11b devices will coexist, and legacy 802.11a/g devices will interoperate with 802.11n devices when operating in the same band and channel. This means 802.11n will need to support 20-MHz channels for backward compatibility. This is important because the survey (Chapter 3) shows increasing use of WLAN devices.

4.5 VLAN – provisions for traffic separation

Virtual local area network (VLAN) is a method of separating users' traffic. To do so, network edge equipment – where users' stations are connected – adds a tag in all the users' originated frames. The rest of the network equipment will treat those frames appropriately taking into consideration the group (VLAN) to which it belongs.

VLAN technology allows network designers to separate the logical connectivity from the physical connectivity. Users are still connected either via physical cables to physical wiring devices or via wireless connections (802.11 a/b/g) to Access Points (in an infrastructure network), but the connectivity view from the application perspective is no longer restricted to the bounds of this physical topology. That is, the LAN is "virtual" in that a set of stations and applications can behave as if they were connected to a single physical LAN when in fact they are not.

Within an electrical substation there may be different types of users and applications. The capability of grouping the users in different VLANs may allow the deployment of different services. For example, company employees/users may require access to the Internet and to their corporate Intranet, and other external users may only be allowed to access to the Internet.

Figure 10 shows a Wi-Fi access point can be configured to serve both types of users. In this example, IEEE 802.1x is the basis for assigning to each user its corresponding VLAN. Authentication servers store user profiles and privileges. In this example, the RADIUS server will configure the Wi-Fi access point to support the VLAN assignments.

This is implemented in the RADIUS message by including an attribute that assigns each type of user to a different VLAN. Based on this information, the Wi-Fi access point will add a tag to all user frames with the corresponding VLAN information. As depicted in Figure 10, traffic is then segregated, and it can subsequently be handled in a different way inside the communications network.

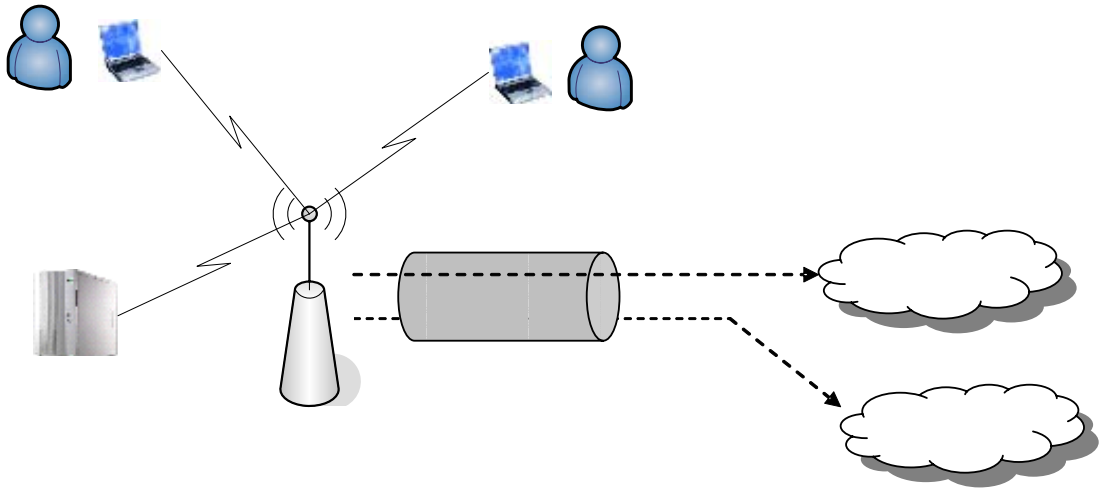

Figure 10 Using VLAN to segregate users

VLAN allows free communication among the members of a given VLAN but does not forward traffic among the members of different VLAN's. VLAN also enhances the Utility's protection against malicious or curious users. Note, users can eavesdrop only on the multicast and unknown unicast traffic within their own VLAN. Similarly, while it is possible to inject malicious traffic, such traffic should only propagate among the members of a certain VLAN, and thus any network disruption will easily be localized.

User1

5. How Wi-Fi access control and information security mechanisms work

As discussed previously, legacy 802.11 security and access control mechanisms are inadequate to protect critical electric utility protection and automation information. In response to the known security weaknesses, IEEE developed 802.11i, which contains the following components.

- IEEE 802.1x for user authentication.
- AES-Counter Mode CBC-MAC Protocol (CCMP) to provide confidentiality, integrity and origin authentication.
- Robust Secure Network (RSN) to keep track of user associations.
  Note: RSN = 802.1X + CCMP = WPA2.

5.1 We begin with IEEE 802.1x

When considering a secure client/host system it is important to ensure that legitimate users are allowed access to appropriate resources and illegitimate users and malcontents are denied access. IEEE 802.1x is designed to authenticate users requesting access to a host using the Extensible Authentication Protocol (EAP). EAP is the authentication framework used to control network access. The EAP framework

provides the capability to negotiate the desired authentication mechanism. Because many authentication schemes exist, EAP is used by the entities to inform each other which scheme is being used.

If you think more is better and you like alphabet soup, you will really like EAP because there are currently about 40 different EAP authentication methods. Many methods are defined in Internet Engineering Task Force (IETF) RFCs. The common EAP methods used in wireless networks include EAP-LEAP, EAP-TLS, EAP-SIM, EAP-AKA, PEAP, and EAP-TTLS.

- EAP-LEAP (Extensible Authentication Protocol - Lightweight Extensible Authentication Protocol) is a proprietary protocol which was developed by Cisco. Cisco is phasing out EAP-LEAP in favor of PEAP.
- EAP-TLS (Extensible Authentication Protocol – Transport Layer Security) was created by Microsoft and accepted by the IETF as RFC 2716: PPP EAP TLS Authentication Protocol.
- EAP-SIM (Extensible Authentication Protocol - Subscriber Identity Module) uses Global System for mobile communications EAP-SIM is described in RFC 4186.
- EAP-AKA (Extensible Authentication Protocol – Authentication and Key Agreement) uses Universal Mobile Telecommunication System. EAP-AKA is described in RFC 4187.
- PEAP (Protected Extensible Authentication Protocol) is a proprietary protocol which was developed by Microsoft, Cisco and RSA Security.
- EAP-TTLS (Extensible Authentication Protocol - Tunneled Transport Layer Security) is a proprietary protocol which was developed by Funk Software and Certicom, and is supported by Agere Systems, Proxim, and Avaya. EAP-TTLS is being considered by the IETF as a new standard.

IEEE 802.1x uses EAP to allow users, or clients, to associate with a host, or service using three roles: supplicant, authenticating server, and authenticator.

- The supplicant is the user, or client, that wants to be authenticated; i.e., supplicant wants access to the host.
- Knowing who is allowed access, the authentication server authenticates the user.
- The device in between the supplicant and the authentication server, such as a wireless access point, is called the authenticator.

The negotiation between the supplicant, authenticating server, and authenticator is shown in Figure 11. In this example, the IED shown in Figure 11 is Programmed Logic Controller (PLC), which relies on the authentication server to authenticate the supplicant before access is granted to the network. This example is shown to illustrate how a secure retrofit solution can be configured.

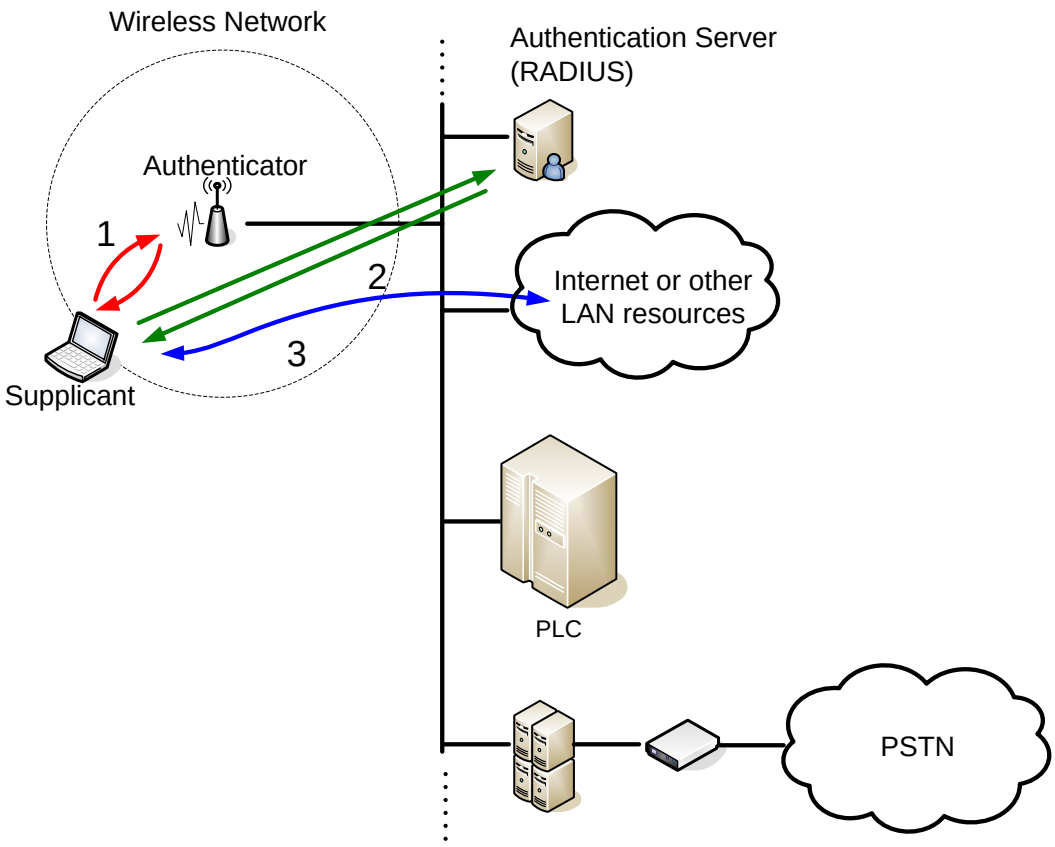

Figure 11 Negotiation between a supplicant, authentication server and an authenticator

The following sequence describes how the supplicant or client gains access to the PLC.

- The supplicant and authenticator negotiate a connection to establish an active link, which associates the suppliant system with the access point. This is similar to the way you associate your computer to a wireless access point in a coffee shop.
- The supplicant sends an “EAP-Response/Identity” packet to the authenticator, which is then passed on to the Authentication Server. This is where the similarity to your coffee shop ends. In the coffee shop scenario, generally you are granted access to the internet or other services without regard to who you are. By contrast, using EAP, a cryptographic authentication request is sent to the access point, which in turn passes the request to the Authentication Server. The Authentication Server is responsible to prove that access to the PLC (host) or other network services is allowed.
- The Authentication Server sends back a challenge to the authenticator. The authenticator unpacks this from IP and repackages it into EAP message, and sends it to the supplicant. Referring to the coffee shop scenario, the user must now prove his identity.
- The supplicant responds to the challenge via the authenticator and passes the response onto the Authentication Server.
- If the supplicant provides proper identity, the Authentication Server responds with a success message, which is then passed onto the supplicant via the authenticator. The authenticator now allows access to the LAN. This is where

during the coffee shop scenario your computer is allowed access to the internet. If authentication fails, the supplicant is denied access.

Returning to the example shown in Figure 11, a technician (the supplicant) needs wireless access to a PLC in a substation. Assuming the PLC is an older model and doesn't have any cryptographic protection, it must rely on the Authentication Server for the needed authentication services and authenticator for access control. This example clearly illustrates that legacy field devices, such as the PLC, can be integrated into a secure wireless network with strong access control mechanisms.

5.2 AES – Counter Mode CBC-MAC Protocol (CCMP)

Section 5.1 described the means to establish secure identity and access control between the supplicant and the network resources shown in Figure 11. To protect the confidentiality of the data exchanged a strong cryptographic protocol is needed. In general the subject of cryptography protocols and their nuances is not readily understood by most utility engineers because these are vastly different technical disciplines. For that matter, most cryptographers do not understand the power system impacts of fault resistance in determining fault type.

If the details described in the rest of Chapter 5 require a more comprehensive understanding of the foundational mathematics, Reference [11] is recommended, with this warning: the reader may continue reading Chapter 5, or skip to Chapter 6.

5.2.1 Why AES

The National Institute of Standards and Technology (NIST) approved the Advanced Encryption Standard (AES) because so far it has proven to be resilient to attack. The cornerstone of 802.11i data protection is an implementation of AES, which is called AES – Counter Mode CBC-MAC Protocol (CCMP) – see [18] . The 128-bit block cipher, as the name implies, encrypts 128 bit data blocks. However, blocks can be combined in various ways to form cryptographic protocols.

AES-CCMP incorporates two sophisticated cryptographic techniques; counter mode encryption and cipher block chaining with a message authentication code - called CBC-MAC and AES-CCMP adapts them to Ethernet frames to provide a robust security protocol between the supplicant and the authenticator.

The AES counter mode provides data confidentiality, and the CBC-MAC provides message integrity. Note: 128-bit AES provides enough security to meet the needs for the NIST Federal Information Processing Standard (FIPS) 140-2 specification. However, as hackers become more sophisticated, we believe that in the future 192- or 256-bit AES may be required in order to provide increased security.

5.2.2 Given AES-CCMP, how should it be implemented

The following discussion describes how AES-CCMP is integrated in IEEE 802.11i to provide data security. AES-CCMP is really quite simple and efficient because it only uses a single type of encryption. The CBC-MAC function is used to calculate a Message Integrity Check (MIC). The AES counter mode is used to encrypt the 802.11 payload (data) and the MIC.

5.2.2.1 CCMP generated frame

The CCMP data frame consists of the elements shown in Figure 12.

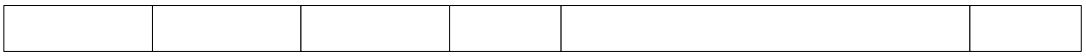

Figure 12 CCMP generated frame

Starting block is a 128-bit block that is described in 5.2.2.2.

MAC header is the 802.11i MAC header with the values of the fields that can change in transit.

CCMP header is 8 bytes and contains the 48-bit Packet number and additional fields.

Padding bytes (set to 0) are added to ensure that the portion of the entire encrypted data block, including the plaintext data, is an integral number of 128-bit blocks.

Data is the plaintext (unencrypted) portion of the 802.11i payload.

Padding bytes (set to 0) are added to ensure that the portion of the MIC data block includes the plaintext data is an integral number of 128-bit blocks.

Unlike data integrity for both WEP and WPA, CCMP (or WPA2) provides data integrity for both the 802.11 header (except changeable fields) and the 802.11i payload.

5.2.2.2 Starting block for MIC calculation

The starting block for the MIC calculation consists of the components shown in Figure 13.

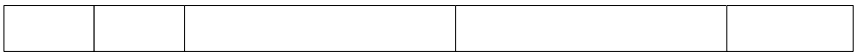

Figure 13 Start block for MIC calculation

Flag (8 bits) is set to 01011001 and contains various flags, such as a flag that indicates that the MIC used in the 802.11i frame is 64 bits long.

Priority (8 bits) is reserved for future purposes and is set to 0.

Source Address (48 bits) is from the 802.11i MAC header.

Packet Number (48 bits) is from the CCMP header.

Data Length (16 bits) is the length of the plaintext data in bytes.

5.2.2.3 Procedure to build a CCMP frame

The first step to build a CCMP frame is to calculate a MIC value, using the following process.

1. Using AES encrypt a starting 128-bit block of data that is to be transmitted and the data integrity key. This produces a 128-bit result (Result1).
2. Perform an exclusive OR (XOR) operation between Result1 and the next 128 bits of the data over which the MIC is being calculated. This produces a 128-bit result (Xresult1).
3. Using AES encrypt Xresult1 and the data integrity key. This produces Result2
4. Perform a XOR between Result2 and the next 128 bits of the data. This produces Xresult2.

Steps 3-4 repeat for the additional 128-bit blocks in the data. The high-order 64 bits of the final result is the CCMP MIC. Figure 14 shows the MIC calculation process.

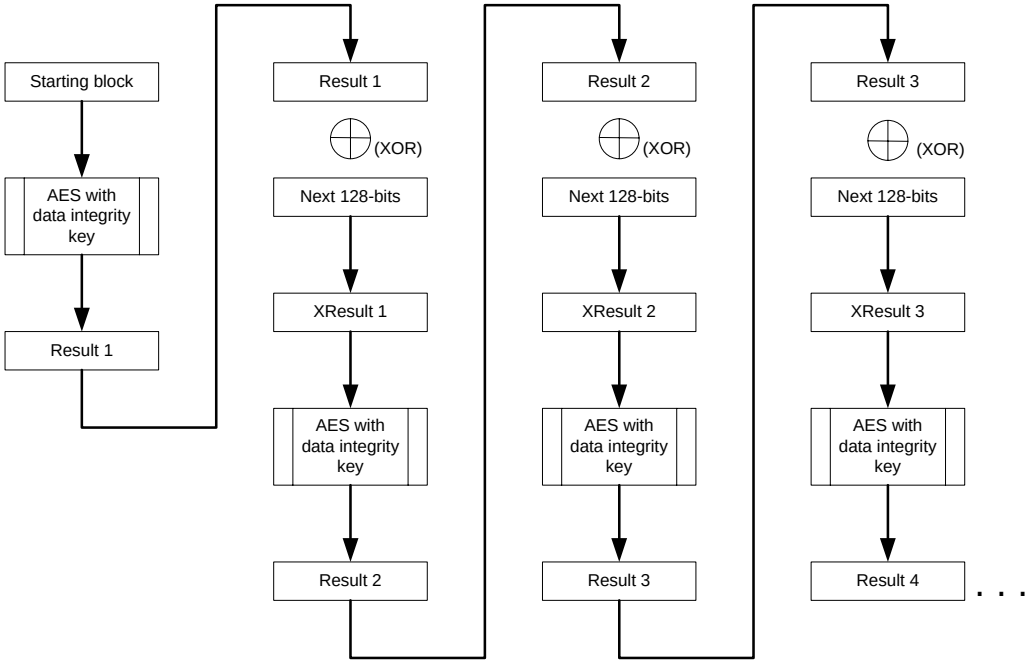

Figure 14 MIC calculation sequence and results

5.2.2.4 AES counter mode calculation

The AES counter mode encryption algorithm uses the following process.

1. Encrypt a starting 128-bit counter with AES and the data encryption key. This produces a 128-bit result (Result1).
2. Perform an exclusive OR (XOR) operation between Result1 and the first 128-bit block of the data that is being encrypted. This produces the first 128-bit encrypted block.
3. Increment the counter and encrypt it with AES and the data encryption key. This produces Result2.
4. Perform XOR between Result2 and the next 128 bits of the data. This produces the second 128-bit encrypted block.

AES counter mode repeats steps 3 and 4 for the additional 128-bit blocks in the data until the final block. For the final block, AES counter mode XORs the encrypted counter with the remaining bits, producing encrypted data of the same length as the last block of data. Each encrypted block is concatenated to form the final encrypted data portion of the CCMP message. Figure 15 shows the AES counter mode process.

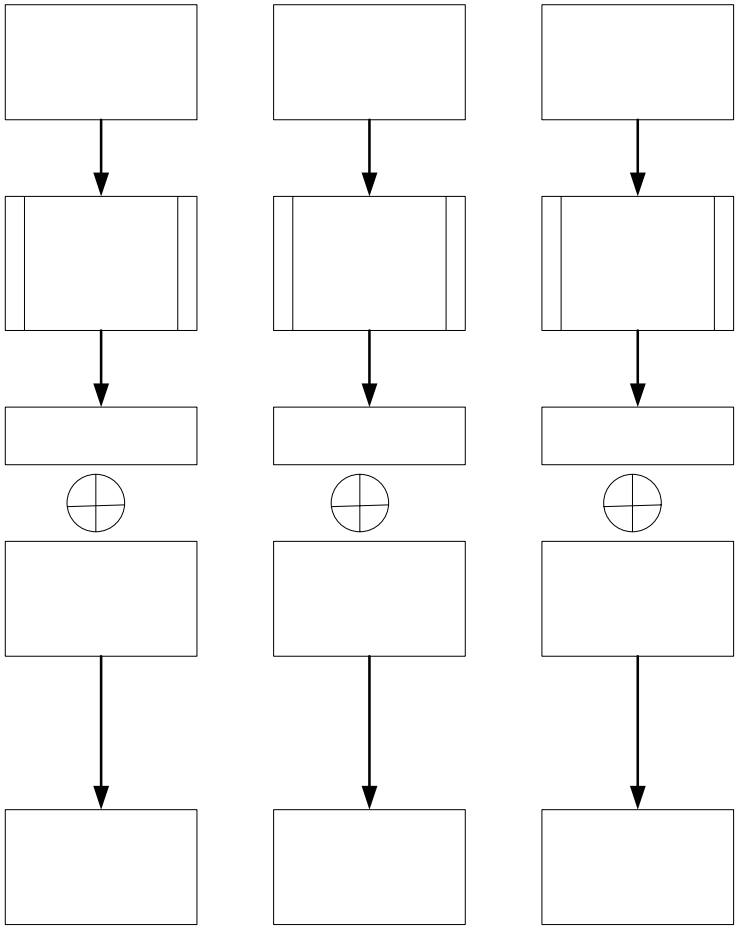

Figure 15 AES counter mode calculation

AES with data encryption key

5.2.2.5 Start value for AES counter mode

The start value for AES counter mode is shown in Figure 16.

Figure 16 Start value for AES counter mode

Flag (8 bits) is set to 01011001, which is the same Flag value that is used for the MIC calculation.

Priority (8 bits) is reserved for future purposes and is set to 0.

Source Address (48 bits) is taken from the 802.11 MAC header.

Packet Number (48 bits) is taken from the CCMP header.

Counter (16 bits) is set to 1 and is only incremented if an 802.11 payload is fragmented into smaller payloads. Note that this Counter field is not the same as the 128-bit counter value used in the AES counter mode encryption algorithm.

Result 1

(XOR

5.2.2.6 How to build the CCMP message

To build the CCMP message frame, CCMP uses the following process.

1. Input the starting block, 802.11 MAC header, CCMP header, data length, and padding fields into the CBC-MAC algorithm with the data integrity key to produce the MIC.
2. Input the starting counter value and the combination of the data with the calculated MIC into the AES Counter mode encryption algorithm with the data encryption key to produce the encrypted data and MIC.
3. Add the CCMP header containing the Packet Number to the encrypted portion of the 802.11 payload, and encapsulate the result with the 802.11 header and trailer.

5.2.2.7 CCMP encryption process

The CCMP process to encrypt a data message is shown in Figure 17.

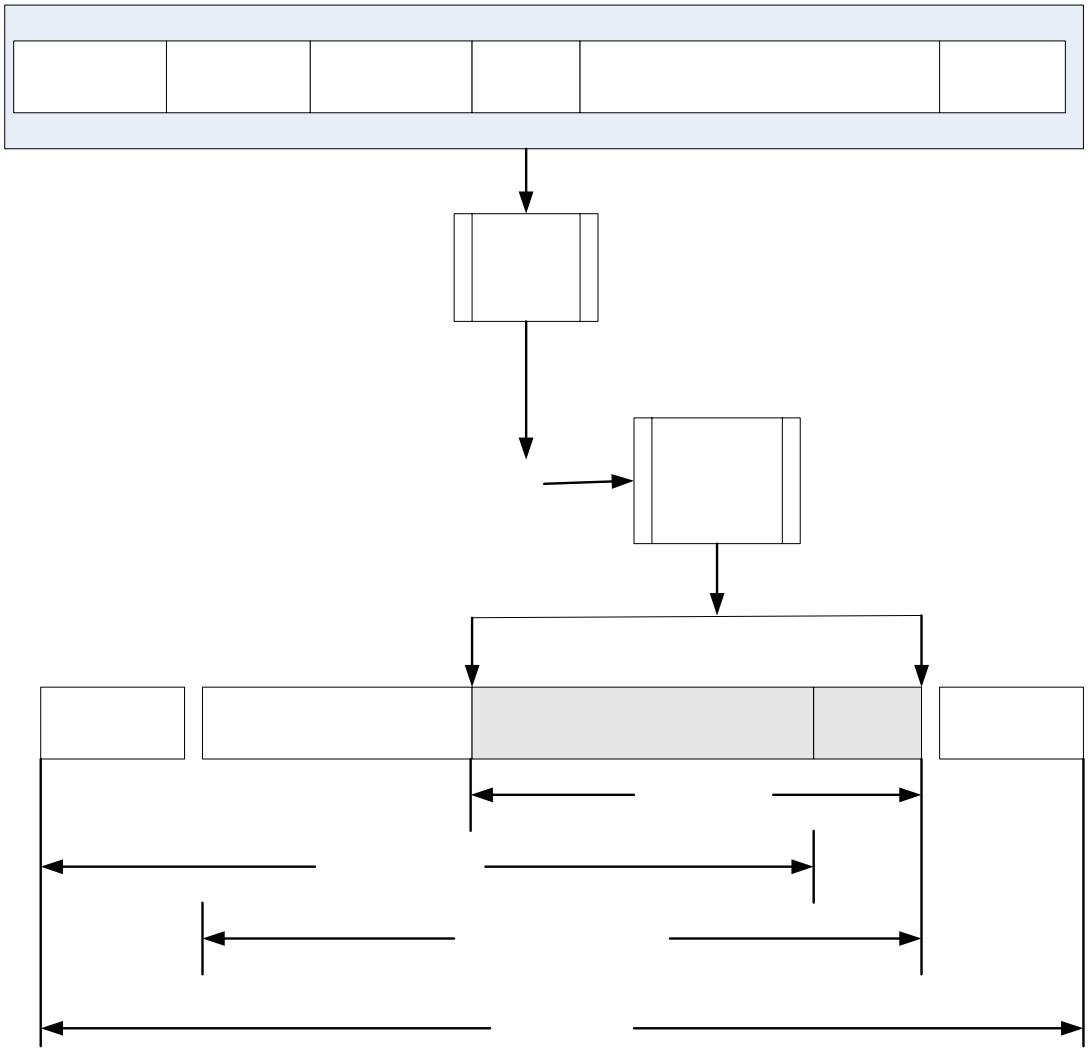

Figure 17 CCMP encryption process for a unicast data frame

5.2.2.8 How the message is decrypted

To decrypt data and verify its integrity, CCMP uses the following process:

1. Determine the starting counter value from values in the 802.11i and CCMP headers.
2. Input the starting counter value and the encrypted portion of the 802.11i payload into the AES counter mode decryption algorithm with the data encryption key to produce the decrypted data and MIC. For decryption, AES counter mode XORs the encrypted counter value with the encrypted data block, producing the decrypted data block.
3. Input the starting block, 802.11i MAC header, CCMP header, data length, and padding fields into the AES CBC-MAC algorithm with the data integrity key to calculate a MIC.
4. Compare the calculated value of the MIC to the value of the unencrypted MIC. If the MIC values do not match, CCMP silently discards the data. If the MIC values match, CCMP passes the data to the upper networking layers for processing.

The CCMP process to decrypt a data message is shown in Figure 18.

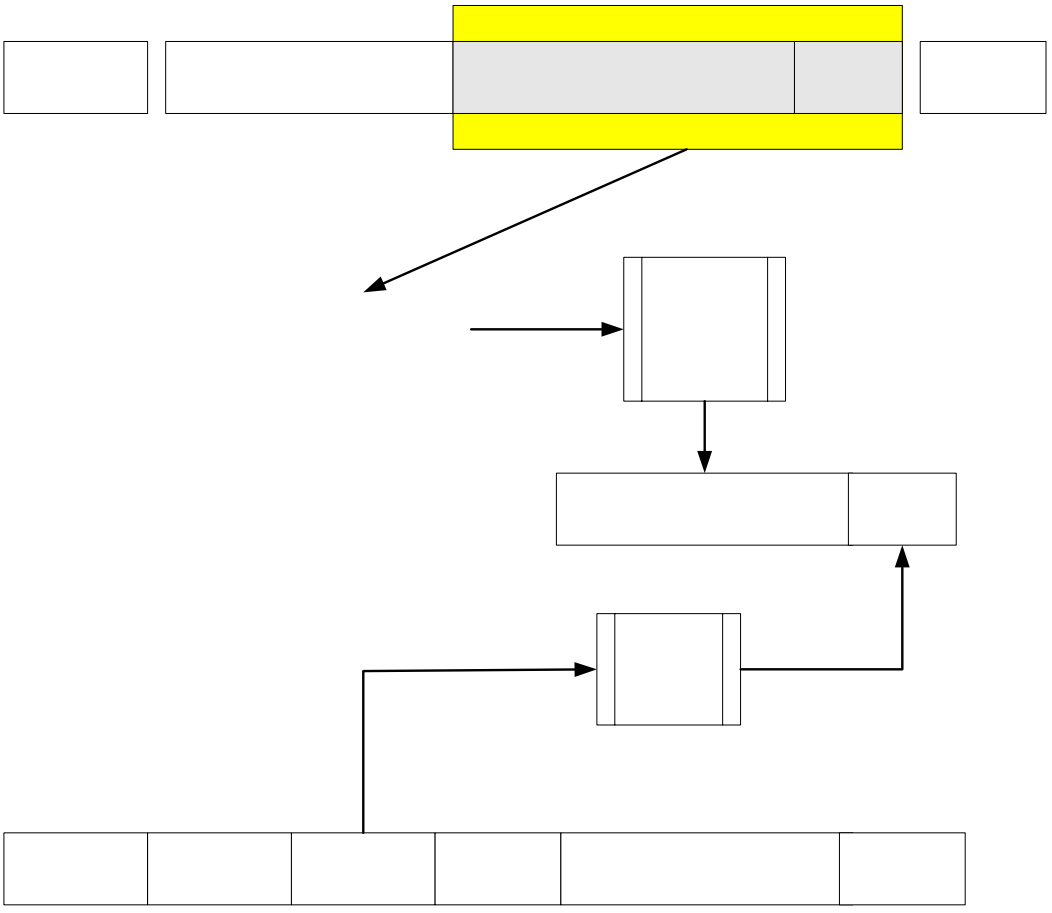

Figure 18 CCMP decryption process for a unicast data frame

5.3 Robust secure network parameters

Robust Secure Network (RSN) is a protocol that dynamically negotiates the authentication and encryption algorithms to be used for communications between wireless access points and wireless clients, establishing secure communications over an 802.11 wireless network. The RSN process is:

1. The wireless client NIC sends a Probe Request.
2. The wireless access point sends a Probe Response with an RSN Information Exchange (IE) frame.
3. The wireless NIC requests authentication via one of the approved methods.
4. The wireless access point provides authentication for the wireless NIC.
5. The wireless NIC sends an Association Request with an RSN Information Exchange (IE) frame.
6. The wireless access point sends an Association Response.

RSN then begins to establish a secure communication channel by broadcasting an RSN Information Element message across the wireless network. The RSN Information Element (IE) broadcasts the following information:

- All enabled authentication suites
- All enabled unicast cipher suites
- Multicast cipher suite

The format of the RSN Information Element frame is shown in Table 4.

Table 4 RSN information element frame

Field	Length in octets
Element ID	1
Element Length	1
Version	2
Group key suite	4
Pairwise suite count	2
Pairwise suite list	4 per pairwise suite
Authentication suite count	2
Authentication suite list	4 per authentication suite
Capabilities	2

Authentication and key management suites supported by RSN are shown in Table 5.

Table 5 Authentication and key management suites supported by RSN

Code	Meaning
00:00:00:1	802.1X authentication and key management
00:00:00:2	No authentication; 802.1X key management

The pair-wise or group cipher suites supported by RSN are shown in Table 6.

Table 6 Cipher suites supported by RSN

Code	Meaning
00:00:00:1	WEP
00:00:00:2	TKIP
00:00:00:3	WRAP
00:00:00:4	CCMP
00:00:00:5	WEP-104

6. Strategy for defense-in-depth

To understand defense-in-depth (DiD), one should start with a high-level understanding of the need to protect a nation's critical infrastructure. Industrial control systems (ICSs) include electric power, gas, oil, water, chemical processing and manufacturing processes. A control center nominally includes access servers, historian servers, local and remote human machine interface (HMI) stations, and communication/networking infrastructure.

More recently, there is a trend to replace specialized control devices with general-purpose (or multi-function) Intelligent Electronic Devices (IEDs) and associated data communication technology. It is most common that parts of the process control networks are interconnected with their corporate intranets. Moreover, ICS are distributed in a metropolitan area where communications media now include Public Switched Telephone Network (PSTN), wireless communications and the Internet. These are potential security vulnerabilities that are associated with each of the communication paths. As wireless LANs are increasingly being introduced in the critical infrastructure, wireless security surfaces is the major concern (see Chapter 3). The most probable reasons for this concern are discussed in this chapter in Section 6.2.

6.1 Defense-in-depth is needed to achieve information assurance

Defense-in-depth offers a practical strategy to achieve Information Assurance[2] (IA) in today's highly connected environments. DiD relies on the intelligent application of techniques and technologies that currently exist as well as enabling the enterprise architecture the flexibility to accommodate future and emerging techniques ant technological components.

This notional concept is highly proactive and future proof because the strategy recommends a balanced look among the physical domain, information domain, and the economy domain covering protection capability and cost, performance, and operational considerations. The balance of this chapter presents an overview of the major components of this strategy.

[2] Information security deals with several different "trust" aspects of information. Another common term is information assurance. Information security is not confined to computer systems, IEDs, or to information in an electronic or machine-readable form. It applies to all aspects of safeguarding or protecting information or data, in whatever form.

6.1.1 Who are the adversaries

The sheer number and sophistication of cyber attacks are endangering every nation's critical infrastructure information networks. At the same time, increasingly these networks are being utilized to plan a role in processing, storing, monitoring and controlling the infrastructural engines of energy, transportation, finance and manufacturing. Disruption of these networks can have a dire consequence on any nation or union of nations.

To defend against attacks on information and information systems, each organization and enterprise needs to comprehend and characterize its adversaries, their potential motivations, and types of attacks. A high percentage of the survey respondents indicated they had no plans for performing a security risk assessment which includes Wi-Fi. They don't understand the problem.

Potential adversaries might include nation states, non-governmental organizations (NGOs), terrorists, criminal elements, hackers, etc. Surveys by EPRI [16] and others have identified the Insider threat as one of the highest intrusion threats in today's environment. Figure 19 shows the results of EPRI's survey of electric utilities reported in Reference [16] .

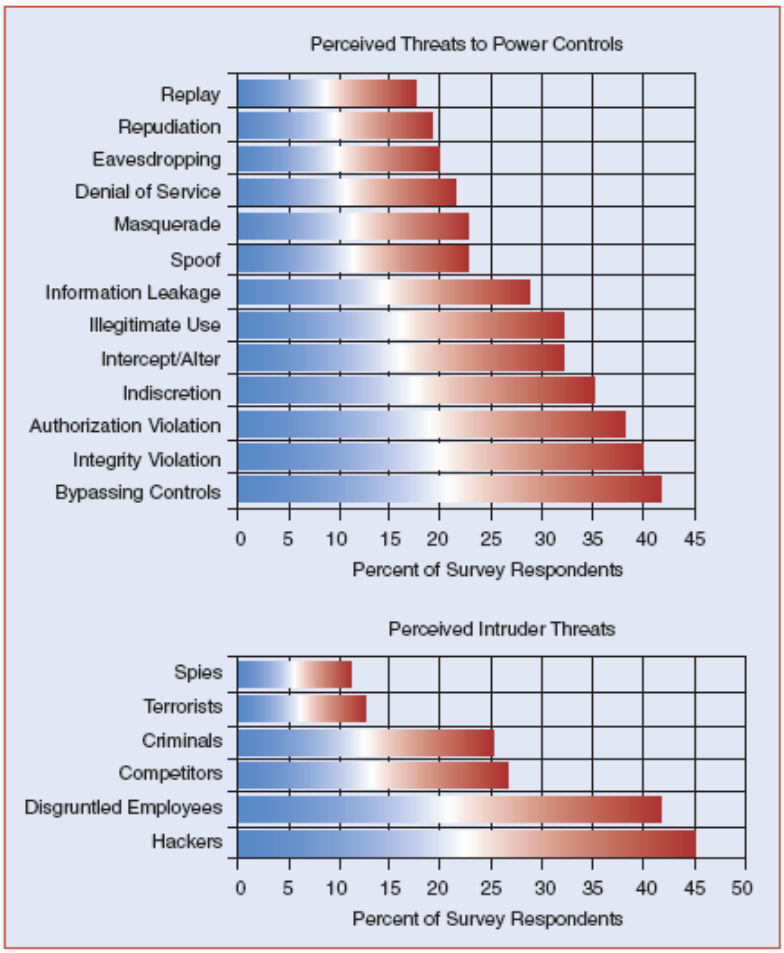

Figure 19 Perceived threats to power supply control: Results of EPRI survey of electric utilities

Clearly, one can deduce from Figure 19 that Identity Management (IM) and Role Based Access Control (RBAC) are required to minimize these threats.

6.1.2 What motivates these people

What motivates these people – just about everything one can imagine? Motivations might consist of intelligence gathering, theft of intellectual property, denial of service embarrassment, or bragging rights in exploiting or defacing a notable target. Attack types might include: passive monitoring, communication network sniffing, active attacks, close-in-attacks, exploitation of insiders, and attacks through the industry providers of the Information Technology (IT) resources.

An intrusion is defined as “any set of actions that attempt to compromise the availability, integrity, or confidentiality of a resource. In process control systems, including electric power transmission and distribution systems, availability is most important. This is quite different than the classic IT mindset, where in office information systems, integrity and confidentiality are more important than availability.

6.2 Type of threat dictates the defense-in-depth strategy

Types of threat can generally be classified into five groups.

6.2.1 Passive eavesdropping and traffic analysis

The adversary can sniff and log the traffic in a WLAN. It then may learn partial or complete information from the aggregate data. If there is a vulnerability, recorded encrypted messages might be used to reveal the encryption key; or might reveal a means towards the decryption of the packets; or, if the key is not made available, might reveal profile useful information using traffic analysis tools.

6.2.2 Active eavesdropping for message interception, deletion and injection

An attacker might be able to intercept, delete, or insert a message into the WLAN using moderate equipment (e.g., a network interface card, relevant software, etc). An adversary is then capable of generating, controlling, modifying and transmitting packets. In the case when data authentication functionality is enforced, the knowledgeable adversary is capable of compromising the data integrity algorithm to create a valid packet. The adversary is also capable of inserting a replayed packet if no replay protection is implemented or the attacker is able to circumvent the replay protection if it is enabled. Moreover, the attacker might be able to gather more information from the system response as an outcrop of active eavesdropping.

6.2.3 Masquerading and malicious access

An adversary can learn valid plaintext Medium Access Control (MAC) addresses by eavesdropping, and can modify its MAC address. If a MAC address is employed as the identification of the wireless system, the adversary can masquerade as a wireless access point by spoofing its MAC address. The attacker can install its own access point, with a forged MAC address and a spoofed service set identifier (SSID). Also, a malicious or rogue access point can provide a strong signal in fooling another wireless station in an association with it and leaking private information. A phishing process can be directed at an authorized user of the utility by means of an official looking e-mail in attempting to gather information about the user. A consequential impact is the loss of the confidentiality of the data. By stealing the credential data of the authorized user, the

attacker might be able to acquire the knowledge to access protected status information. The attacker can later leverage this information for a devious purpose.

6.2.4 Denial of service

Denial of service attacks are designed to deny access to specific communication resources. In WLAN, this includes the disablement of the Basic Service Set (BSS) or disrupting the connection between legitimate and intended users. The adversary may choose to leverage vulnerability or design flaws such as a protocol weakness, unprotected management and control frames, repeated sending of de-authenticated and de-associated frames, and jamming the RF frequency. The severity of the attack depends on the importance of the target resource, the minimum service requirements and the duration of the attack. It is also important to consider the cascading effect with other systems or services depending on the attacked service.

6.2.5 Viral infection and propagation

Viral infection is pretty pervasive in a highly networked environment – it is the equivalent of the pandemic “bird flu.” Virus can be transmitted by an innocuous interaction with an external source, and it can mutate into other forms as it is transmitted from one entity to another. Diligent enforcement of “Patch Management” is not an option, it is an absolute necessity.

6.3 What should be done to mitigate these types of attacks

Information assurance is achieved when information and information systems are protected against attacks. These attacks might be characterized by an application of security services to include availability, integrity, authentication, confidentiality, non-repudiation, authorization, access control, and infrastructure management. These applications should be based on the Protect, Detect, and React (PDR) paradigm. PDR implies that the organization and enterprise needs to expect attacks and erect defense mechanisms to react and recover from these attacks.

An important premise is that the DiD strategy will work, if the enterprise or organization can harmonize these key entities: people, technology and operations.

6.3.1 Its time for the leadership to step up to the plate

If one believes the implication of the survey results reported in Section 3, the leadership of 58% of utilities that have not performed a risk assessment, which includes Wi-Fi, and do not plan to do so is a concern. In light of the wide spread interest in 802.11i and the cost effectiveness of using Wi-Fi, this decision should be reconsidered.

Achieving information assurance starts with the commitment of senior level management to clearly understand the threat. This can be achieved with the technical staff raising the awareness of the threats and their dire consequences. This is followed through establishing and enforcing effective information assurance policies and procedures, role assignment, responsibilities, personnel training, and accountability.

6.3.2 No excuses – the technology is available

There is a wide range of technologies for providing information assurance services and for system assurance. To ensure that a right mix of technologies is deployed, the organization should establish effective policy and processors for acquiring the needed security technology. DiD principles include:

- Defense in multiple places
- Layered defenses
- Specify the security robustness
- Deploy robust and scalable key management
- Deploy a proactive defensive infrastructure

6.3.3 Operations is the front line – the first responder

It is necessary that operations maintain an up-to-date security policy. The policy should require that accredited testing laboratories validate the security functions in all IEDs and add-on devices that provide communication to critical information sources. Operations should have and enforce a disaster recovery and business continuity plan to recover quickly back to operations.

6.4 What defense-in-depth technologies are needed

In general, the security requirements for a WLAN include:

- Availability and timely response to events
- Data confidentiality
- Data integrity
- User authentication
- Access control and permission
- Key management
- Audit logs and supporting forensic evidence

It is tempting to separate security components such as the user authentication, data integrity, and protection. However, such action would weaken the DiD security paradigm. It is important that a security context be maintained to assure information security in a DiD context. The following discusses selected security requirements and their DiD information security alternatives.

6.4.1 Availability is most important

The intended purpose of this technical brochure is to address Wi-Fi usage for securely accessing the protection and automation functions. However, availability is not emphasized as a primary objective of Wi-Fi. Offline WLAN operations such as re-keying and de-authentication can be detrimental in meeting the availability objective.

Since the management frames and control frames are not well protected in a WLAN and are highly susceptible to DoS attack, it is necessary to adopt a central manager to handle these frames and identify forged frames by their aberrant behavior. This will require an authentication server to keep track of all supplicants (i.e., all entities that want to gain access) – see Chapter 7.

6.4.2 Don’t neglect confidentiality and integrity

Confidentiality is the property by which information is made unavailable and not disclosed to unauthorized individuals, entities, or processes. Integrity guarantees that a received message has not changed from the original message.

Because of known Wi-Fi vulnerabilities, data confidentiality and integrity might be problematical and should be addressed as a significant security concern. There are three WLAN data confidentiality protocols: WEP, TKIP, and Counter-mode/Chain Block Cipher with Message Authentication Code (CBC MAC) (CCMP) protocols.

WEP and TKIP use the RC4 stream cipher. WEP has had known security problems which include: static WEP keys, poor initialization vector (IV), no cryptographic integrity protection (i.e., cyclic redundancy check or CRC for packet integrity assurance). The CCMP uses the CCM (counter with CBC-MAC) or the AES. CCMP uses the counter mode for data confidentiality and CBC-MAC for data integrity.

Another alternative is Robust Security Network (RSN) which offers limited-life keys, and temporal and session keys. TKIP is not recommended, the preferred solution is RSN – see Chapter 5[3].

6.4.3 Without access control and permission you're not secure

Wi-Fi security mechanism consists of access control and access permission. It can be divided into user authorization and authentication of identity. A strong Identification and Authentication (I&A) process can be implemented only if the authorization and authentication are vetted together.

User access control can be enforced based on roles, or role based access control (RBAC). A cryptographically binding of the relationships between a user and his assigned role further enhances the identification and authentication process. Different user permissions or credentials are used to denote access level, role assignment, job responsibility, etc.

Credentials can be stored in a secure token such as a smart card, USB fob, or other devices. The inclusion of a biometric evolves into a multi-factor I&A process. For example, a three-factor I&A process consists of what-you-know (user identification or password), what-you-have (token), and what-you-are (biometric).

6.4.4 Without robust key management you have a management nightmare

Critical information security and information management are complicated by today's vastly networked world. The need to identify authorized users, protect and control sensitive information assets, and restrict access to information in compliance with privacy statures and regulations has never been greater. A standard-based, object level, source data centric protection enterprise-wide key management is the answer.

Such a robust key management scheme would allow users to control anything that could be named, from a substation, IED, RTU, PLC, retrofit cryptographic module, historian data or file, or any data repository – see Figure 20.

In addition, RBAC technique can be used to enforce who should be able to see which piece of data through cryptography. Desirable parameters should include, as examples, dynamic key generation, full life-cycle support, and ease of re-keying.

6.4.5 Timely reaction requires intrusion detection and prevention

An intrusion detection system (IDS) generally detects an intrusion and alerts a system administrator without taking further action. Types of detection system are: signature and

[3] TKIP works over the top of WEP offering stronger security than WEP. TKIP is not required when 802.11i is implemented because RSN/CCMP offers stronger security than WPA/TKIP at the lower layers where data is encrypted and decrypted.

anomaly. Signature detection systems search for activities which do not fit predefined patterns. Anomaly detection systems search for unusual or anomalous activities.

An intrusion prevention system (IPS) detects an intrusion, alerts the system administrator, and takes a predefined action (breaking the connection, blocking access) to defend against an attack. To be effective, one must define normal behaviour, and the IPS must provide attack discovery and assessment capabilities, with adaptive anomaly detection to discover and detect emerging threats.

For an IDS/IPS to be effective, it can be based in the host or network, or it can be embedded with a firewall.

6.4.6 Audit logs and supporting forensic evidence

Audit logs are currently in use by about 40% of North American electric power utilities and by about one third of international utilities. Across the world, use of audit logs for control systems operations are estimated to have been implemented in operational control systems at more than 60% of large utilities serving more than 500,000 customers.

In operational control centers or communications security environments audit logging provides a chronological record of system activities to enable the reconstruction and examination of the sequence of events and/or changes in an event**.**

7. What needs to be considered to manage Wi-Fi security

There are many Wi-Fi security management schemes that can be deployed. From discussions with utility executives responsible for security management we must temper any Wi-Fi management scheme to ensure it is an extension of their corporate policy. Utilities do not want stove pipe solutions; they want a comprehensive solution with extensions for each security technology that is balanced with operational constraints.

Given the potentially pervasive use of Wi-Fi (see Chapter 3), a standards-based solution is strongly recommended. First, we need to examine what needs to be managed, and then we need to identify those standards that best fit this need. To address these questions, we used the foundational information described in [1]

7.1 What Wi-Fi security components need to be managed

This chapter addresses the foundational requirements for managing access control, and limited life keys are an important component of these requirements.

7.1.1 Access control is what needs to be managed

One cannot achieve effective Wi-Fi security unless a mechanism is deployed to control who has access and who doesn't have access permissions. There are really two parts to this requirement: Authentication of the identity of who is requesting access, and Authorization or "use permission" if access is granted. Wi-Fi authentication of identity is addressed in this technical brochure. Use permission is not addressed because it is a local matter that requires embedded functionality of the end-device connected to the Wi-Fi access point.

All situations have the following elements:

- An entity that wants to have access – the **supplicant**
- An entity that controls the access gate – the **authenticator**

- An entity that decides whether the supplicant is to be admitted – the **authorizer**

The procedure to authenticate a supplicant is very straight forward.

1. Authenticator is alerted by the supplicant
2. Supplicant identifies itself
3. Authenticator requests authorization from the authorizer
4. Authorizer indicates YES or NO
5. Authenticator allows or blocks access

The supplicant needs a "token" that proves that it has been authorized. It is this token and its digital signature that needs to be managed.

7.1.2 Context is defined by limited-life keys

The 802.11i developers wanted to develop a scaleable security solution that provided protection against all known passive and active attacks. The first and most important change from earlier versions of 802.11 was the separation of the user authentication process and message protection (integrity and privacy)[4]. However, the two parts must be linked together into a "security context." The concept of security context is one of the most important foundational concepts for RSN.

A lot of the architecture relates to how to establish and maintain a security context between the wireless LAN devices (usually a mobile device and an access point). The backbone of this context is the "secret key" upon which security heavily relies.

In RSN the security context is defined by the possession of limited-life keys.

In RSN there are many different keys forming the key hierarchy, and most of these keys are not known before the authentication process completes. In fact, the creation of keys is done in real time as the security context is established, after authentication. These are known as **temporal keys**. These temporal keys may be updated from time to time, but they are always destroyed when the security context is closed.

A key is basically a shared secret between two or more parties. A key can be used in two distinct ways. They can provide proof of your identity and they can give you access to services. During the authentication phase, you prove your identity by demonstrating you have knowledge of a secret. In RSN correctly authenticating enables you to receive or create the keys that are used for encryption and data protection. These are sometimes called the **temporal** or **session keys** because they work only so long as the security context is in place.

Authentication is based on some shared secret that cannot be created automatically. An authentication key must be created by someone trusted and attached to the holder in such a way that it can't be easily copied or stolen. And of course, the trusted key giver has to be certain of the identity of the key receiver. The basis for all authentication methods is the entity to be authenticated possesses some special information in advance, which is called the **master key**. As a general rule, the master key is rarely, if ever, used directly; instead, it is used to create t**emporal keys**.

[4] Authentication is the process by which you prove that you are eligible to join a network (and that network is legitimate); and message protection ensures that once you have joined the network, you can communicate without risk of interception, modification, or other security risks.

7.1.3 Look at the big picture to understand the context for security management

Figure 20 is a notional high-level picture of what is needed to manage security in the context of power system operations. This approach includes a firewall, including a demilitarized zone (DMZ) when required, controlling the flow of information between a Security Management Center (SMC) and other business functions. A state-full firewall will effectively implement “the principle to deny everything not-specifically-allowed.” All these functions need keying material.

Although a DMZ is shown in Figure 20 its implementation can be very complex and is well beyond the scope of this study. It is included only to raise the awareness that some attention should be given to implementing a DMZ to protect the critical components and information that resides in the SMC.

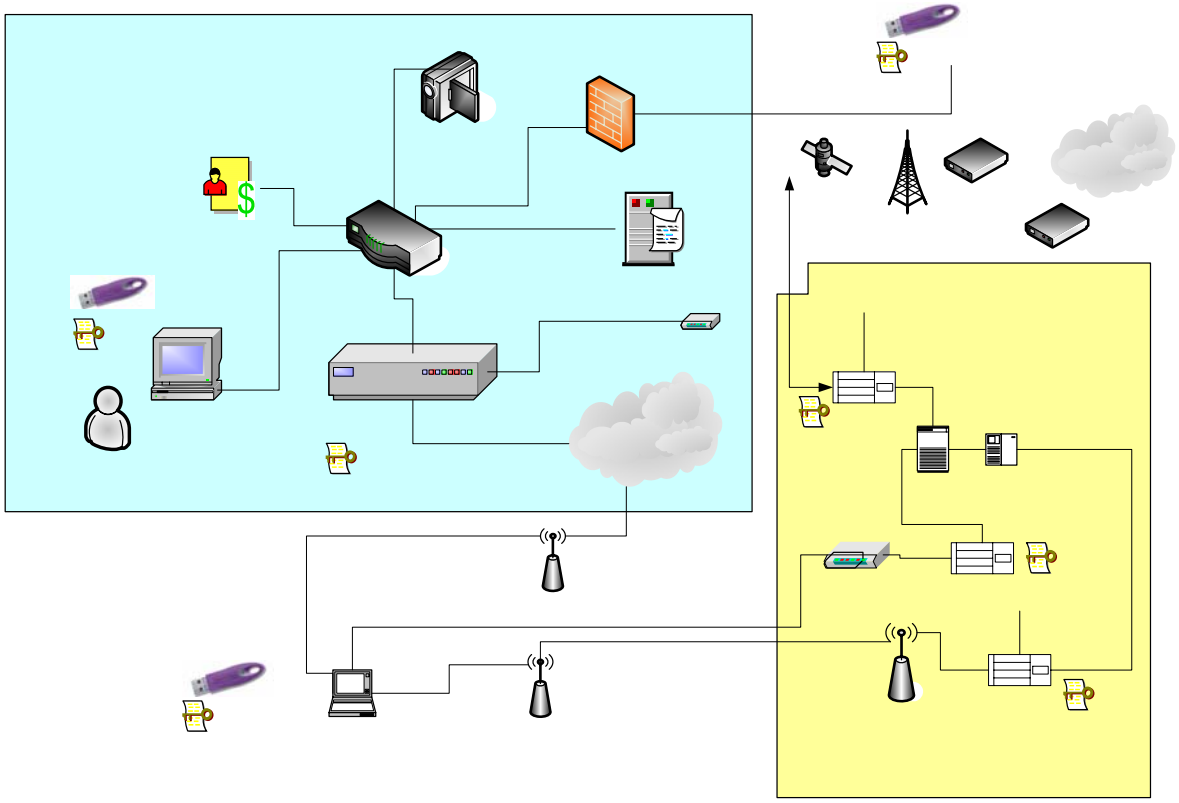

Figure 20 Strong security management is needed for power system operations

SCADA communications between the control center and substation also need to be protected. However, the solution is different depending on whether the communications is over satellite, radios, leased lines, Internet, or the utility’s Intranet[5]. Commonly, leased lines are used, which means SCADA communications need to be protected by in-line SCADA Cryptographic Modules (SCMs) such as those described in AGA 12 – see [2] . These SCMs also need keying material.

[5] Two Internet Engineering Task Force (IETF) Request for Comment (RFC) are of particular interest for Wi-Fi applications See RFC 3610 [3] and RFC 4309 [4] .

Within the substation, Intelligent Electronic Devices (IEDs) such as Remote Terminal Units (RTUs) and protection relays need to be protected against unauthorized entry and operation via the maintenance ports on these field devices. Dial-up to answering modems is very common and needs to be protected.

Wi-Fi users located outside the substation fence or from a stand-off position to IEDs that are difficult to access because of terrain or environmental situations need strong access control mechanisms. Defense-in-depth can be achieved by including a Maintenance Cryptographic Modules (MCM). MCM can be placed in-line between the answering modem and the IED maintenance port or between the Wi-Fi access point and the IED maintenance port. MCMs are described in AGA 12 – see [2] . These MCMs also need keying material.

CIGRE B5.22 gave special attention to the field technician using Wi-Fi to access the maintenance ports of field devices. From a security management point of view the keying material needed by the field technician applies equally well to the dial-up situation. Field Technician is used in the broad sense; it can be a utility employee or an affiliate (relay vendor). These employees and affiliates, according to [16] , are insiders and the utility needs to mitigate the insider threat by managing access and use control under the principle of least privilege.

7.2 Security management – this is the hard part

Figure 20 shows the components needed to create keys, remove keys, and distribute keys. The Admin Network is an isolated local area network within the SMC, which is a physically-secured access facility. Video surveillance is provided to monitor all activity within the SMC as well as access to the SMC.

The software licensing key server shown in Figure 20 is a centralized system which provides tokens, or keys, to client systems in order to enable licensed software to run on them. It is the job of a software licensing key server to make sure that only as many copies of a software package that have been licensed by a customer are allowed to be run at one time.

Typically, a large corporate enterprise will deploy a dedicated machine to perform as the key server. However, the server component of a client server application may also contain an internal licensing key server. Key servers are more commonly used for industry specialized applications than for common applications due to the complexity of their management.

Also shown in Figure 20 is the auditing function to perform an evaluation of an organization, system, process, or product. To be effective, the auditing function must be performed by a competent, objective, and unbiased person or persons, known as auditors. The auditor’s purpose is to verify that the subject of the audit was completed or operates according to approved and accepted standards, statutes, regulations, or practices. Results of the audit should also be used to evaluate controls to determine if conformance is adequate.

Distribution of key materials uses a proxy server. The proxy server shown in Figure 20 is a computer network service that allows clients to make indirect network connections to other network services. A client connects to the proxy server, requests a connection, file, or other resource available on a different server. The proxy provides the resource either by connecting to the specified server or by serving it from a cache. In some cases, the proxy may alter the client’s request or the server’s response for various purposes. A proxy server can also serve as a firewall.

Lastly, in Figure 20 is the Certificate Authority (CA). In cryptography, a certificate authority is an entity which issues digital certificates for use by other parties. It is an example of a trusted third party. CA's are characteristic of many public key infrastructure (PKI) schemes. There are many commercial CAs that charge for their services. Institutions and governments may have their own CAs, and there are many free CAs.

A CA will issue a public key certificate which states that the CA attests that the public key contained in the certificate belongs to the person, organization, server, or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users (relying parties) can trust the information in the CA's certificates. The usual idea is that if the user trusts the CA and can verify the CA's signature, then they can also verify that a certain public key does indeed belong to whoever is identified in the certificate.

If the CA can be subverted, then the security of the system breaks down. This is an issue that must be addressed in a future paper.

The problem of assuring correctness of match between data and entity when the data are presented to the CA (perhaps over an electronic network), and when the credentials of the person/company/program asking for a certificate is likewise presented, is difficult. For this reason, commercial CAs often use a combination of authentication techniques including leveraging government bureaus, the payment infrastructure, third parties databases and services, and custom heuristics. In some enterprise systems, local forms of authentication such as Kerberos can be used to obtain a certificate which can in turn be used by external relying parties. Notaries are required in some cases to personally know the party whose signature is being notarized; this is a higher standard than can be reached for many CAs.

In complex, large-scale deployments, Jerry may not be familiar with Bob's certificate authority (perhaps they each have a different CA), so Bob's certificate may also include his CA's public key signed by a different CA, which is presumably recognizable by Jerry. This process typically leads to a hierarchy or mesh of CAs and CA certificates.

Hierarchical closed-systems are well understood and codified in existing standards – see ANSI X9.69 [5] . But, a utility may have need to implement a federated system to include partners, vendors, government agencies, regulatory agencies each of which has their own CA. Such a federated scheme needs more research and standardization to ensure that reasonable level of interoperability is achieved between these independent organizations.

7.3 What standards best fit the need for effective Wi-Fi security management

Three protocols are used to implement access security in WPA and RSN: IEEE 802.11X, EAP, and RADIUS. The first two protocols are mandatory for WPA and RSN. RADIUS is the method of choice for WPA and is an option for RSN.

8. Substation environmental considerations

Most Wi-Fi networking equipment found at commercial retail stores, like Radio Shack or Wal-Mart, are designed to operate in offices or homes where the temperature and other climatic conditions are held fairly constant. This is a reasonable design guideline for these sorts of equipment because they occupy the same surroundings as people and we like the temperature at 20°C and 35% relative humidity. However, substation and

industrial environments are very different than the comfort of your home. Substation and/or industrial environments include:

- Extreme temperature ranges
- High humidity
- High electrical noise environments including Radio Frequency Interference (RFI) and electrical transients both radiated and conducted.
- High magnetic field
- If mounted near machinery, vibration and shock exist.

Equipment applied in these sorts of applications must be able to operate in conditions that are much more punishing than an air-conditioned server room or a home office.

The CIGRE B5.22 working group recognized that commercial equipment is not suitable for applications in substation environments. Our choice would be to reference either IEC or IEEE standards to help the reader determine what minimum environmental capabilities Wi-Fi equipment should have to meet. However, most IEC standards were developed for protective relaying (in IEC parlance – measuring relays) so one of the test criteria is in essence “no false trips”. There is no requirement for testing a communication device. This situation was recognized when the IEEE WG on IEEE 1613 adapted the IEEE PSRC relay standards (IEEE C37.90, 90.1, 90.2 and 90.3) to a communications environment and a communication test was defined but not for Wi-Fi equipment. Though most IEEE and IEC electrical and environmental test standards are very similar there are differences. For example IEC RF immunity only requires testing to 10 volts per meter level. The US and Canadian utilities were concerned with RF induced false trips, and for this reason they revised IEEE C37.90.2 to require 35 volts/meter immunity.

Because there are no official IEEE or IEC Wi-Fi test standards to reference, a reasonable approach is to extend the IEC concept of “no false trips” to our technical brochure as “no undesirable operations.” That is, when a Wi-Fi device is in service and subjected to external environment influences, the Wi-Fi device does not behave in an unintended manner, such as becoming inoperable or being permanently damaged. To this end we purposely will avoid referencing specific IEEE or IEC standards but will recommend the intent of standards.

Below are minimum environmental and electrical tests that a substation Wi-Fi system should meet. The user should take care to ensure that the Wi-Fi device meets the environmental conditions in which it will be installed and that the Wi-Fi device also meets applicable local governmental requirements (e.g. RF power limits, frequency bands, etc.).

Table 7 Minimum environmental and electrical test required for Wi-Fi equipment

Environmental	Temperature: –40° to +75°C Humidity: 5 to 95% humidity (non-condensing)
Electrical	RFI: 35 V/m ESD: 8 kV contact discharge, 15 kV air discharge Fast Transient: 4 kV
RF Certifications	FCC Part 15.247 IC ECES-003, RSS-210

A. References

[1] Real 802.11 security – Wi-Fi protected access and 802.11i, John Edney and William A. Arbaugh, Addison-Wesley, 2004.

[2] AGA Report Number 12, Part 1, “Cryptographic Protection of SCADA Communications” – General Requirements.

[3] IETF RFC 3610 “Counter with CBC-MAC (CCM),” September 2003.

[4] IETF RFC 4309 “Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP),” December 2005.

[5] ANSI X9.69-1994, “Framework for Key Management Extensions”

[6] IEEE 100: “The Authoritative Dictionary of IEEE Standard Terms”, Seventh Edition.

[7] Krawczyk, H. M. Bellare, and R. Canetti. 1997. HMAC: Keyed-Hashing for Message Authentication. Technical Report RFC 2104. IETF.

[8] Borisov, N, I. Goldberg, and D. Wagner. 2001 Intercepting mobile communications: the insecurity of 802.11. In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking. Pp. 180-188.

[9] Walker, J. 2000. Unsafe at any key size; and analysis of the WEP encapsulation. IEEE 8-2.11-00/362.

[10] Fluhrer, S., I Mantin, and A. Shamir. 2001 Weaknesses in the key scheduling algorithm of RC4. In Eighth Annual Workshop on Selected Areas in Cryptography.

[11] Menezes, Alfred J., van Oorschot, Paul C., and Vanstone, Scott A. (1997) Handbook of Applied Cryptography, CRC Press. Note: Menezes, et al, provide a readable discussion on the details of many areas of cryptography and attacks, but this book also pre-dates AES.

[12] IEEE Std 1646™-2004: IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation.

[13] IEEE Std C37-115™-2004: Standard Test Method for Use in the Evaluation of Message Communications between Intelligent Electronic Devices in an Integrated Substation Protection, Control and Data Acquisition System.

[14] IEC 61850, 2003/2004: Communication Networks and Systems in Substations.

[15] http:www.deviceforge.com/articles/AT5096801417.html by James M. Wilson, Communications Technology Lab, Corporate Technology Group.

[16] IEEE Power & Energy Magazine, September/October 2004 “The Future’s Smart Delivery System” by Clark W. Gellings, Marek Samotyj, and Bill Howe

[17] NIST Special Publication 800-97 (Draft), Guide to IEEE 802.11i: Establishing Robust Security Networks

[18] Microsoft TechNet: http://www.microsoft.com/technet/community/columns/cableguy/cg0805.mspx

[19] Newton-Evans Research Company study, January 2006 "The World Market of SCADA, Energy Management Systems and Distribution Management Systems in Electric Utilities: 2005-2007. Study is available from www.newton-evans.com.

B. Definitions and acronyms

B.1 Definition of terms

Asset	A useful or valuable quality, person, or thing; an advantage or resource.
Authentication	The process by which you prove that you are eligible to join a network
Authenticator	An entity that controls the access gate
Authorization	Access privileges granted to an entity; conveys an "official" sanction to perform a security function or activity.
Authorizer	An entity that decides whether the applicant is to be admitted
Availability	A process that ensures that information or resources are available when required.
Cipher Block Chaining	Cryptographic technique where each block of plaintext is XORed with the previous cipher text block to form the new encrypted block
Cisco Key Integrity Protocol	A proprietary implementation of 802.11i
Confidentiality	Mechanisms that protect protects against the inadvertent or malicious disclosure of sensitive information
Counter Mode	An encryption mode that generates the next keystream block by encrypting successive values of a "counter. The keystream is then XORed with the plaintext block to produce the encrypted block.
Cryptography	The study of making and breaking encryption algorithms
Entity	An individual (person), organization, device or process.
Information assurance	See information security
Information security	Mechanisms that deal with several different "trust" aspects of information as it applies to all aspects of safeguarding or protecting information or data, in whatever form. Another common term is information assurance.
Integrity	The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
Message protection	A process to ensure that once you have joined the network, you can communicate without risk of interception, modification, or other security risks
Non-repudiation	A service that is used to provide proof of the integrity and origin of data in such a way that the integrity and origin can be verified by a

	third party as having originated from a specific entity in possession of the private key of the originator.
Password	A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.
Phishing	A form of criminal activity using social engineering techniques. It is characterized by attempts to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Phishing is typically done using email or an instant message. The term *phishing* arises from the use of increasingly sophisticated lures to “fish” for users’ financial information and passwords.
Proxy server	A process providing a cache of items available on other servers which are presumably slower or more expensive to access.
Revocation	The state of being cancelled or annulled.
Supplicant	An entity that wants to have access
Wi-Fi	An industry standard for products based on IEEE 802.11 as defined by the Wi-Fi alliance – an industry consortium

B.2 Definition of acronyms

ACL	Access Control List
AES	Advanced Encryption System
AKA	Authentication and Key Agreement
BSS	Basic Service set
CA	Certificate Authority
CBC	Cipher Block Chaining
CCMP	Counter Mode CBC-MAC Protocol
CKIP	Cisco Key Integrity Protocol
DMZ	Demilitarized Zone
DoS	Denial of Service
DiD	Defense in Depth
EAP	Extensible Authentication Protocol
EPRI	Electric Power Research Institute
ESD	Electro Static Discharge
HMAC	Hashed Message Authentication Codes
HMI	Human Machine Interface
IA	Information Assurance
IC	Integrated Circuit
IM	Identity Management

ICS	Industrial Control System
IED	Intelligent Electronic Device
IETF	Internet Engineering Task Force
ISM	Industrial, Scientific, Medical
ISO	International Organization for Standardization
IT	Information Technology
kHz	Kilohertz
LEAP	Lightweight Extensible Authentication Protocol
MAC	Message Authentication Code or Media Access Control
MCM	Maintenance Cryptographic Module
MD5	Message Digest 5
MHz	Megahertz
MIC	Message Integrity Check
MIMO	Multiple-Input Multiple-Output
NIC	Network Interface Card
NIST	National Institute of Standards and Technology
OTA	Over The Air
PAR	Protect, Act and Respond
PEAP	Protected Extensible Authentication Protocol
PHY	Physical Layer
PKI	Public Key Infrastructure
PLC	Programmed Logic Controller
PSTN	Public switched telephone network
RADIUS	Remote Authentication Dial-In Service
RBAC	Role Based Access Control
RFC	Request for Comment
RFI	Radio Frequency Interference
RSN	Robust Security Network
RTU	Remote Terminal Unit
SAP	Service Access Point
SCM	SCADA Cryptographic Module
SDM	Spatial Division Multiplexing
SIM	Subscriber Identity Module
SMC	Security Management Center
SSID	Service Set Identifier

TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TSN	Transitional Security Network
TTLS	Tunneled Transport Layer Security
VLAN	Virtual Local Area network
VPN	Virtual Private network
WAP	Wireless Protected Access
WAPI	Wired Access Protected Infrastructure
WEP	Wired Equivalent Privacy
WEP-104	Choice of encryption key (sometimes called 128-bit)
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access

C. Known attacks against Wi-Fi

Unfortunately, none of the original security mechanisms in IEEE 802.11 were robust. Adversaries easily bypass both the access control mechanisms and the shared-key authentication mechanism. Serious flaws in the WEP encapsulation process allow recovery of the secret encryption key and the malicious modification and replay of WEP-protected datagrams. Each of these problems alone poses a significant threat – together, they make exploiting 802.11 networks easy.

Fortunately, both WPA and RSN in IEEE 802.11i prevent the confidentiality, integrity, and access control attacks. Unfortunately, however, neither WPA nor RSN prevents denial-of-service attacks using forged management frames.

Known attacks against Wi-Fi are classified into four broad categories: snooping, modification, masquerading and denial-of-service. This appendix describes these attacks in terms of the security mechanism that they break.

C.1 An overview of the security mechanisms under attack

The basic security mechanisms under attack are confidentiality, integrity, and availability.

C.1.1 Confidentiality

Confidentiality protects against the inadvertent or malicious disclosure of sensitive information. Usually, confidentiality is provided by cryptographic or access control mechanisms.

Encryption is the process of making information indiscernible to an adversary, and cryptography is the study of making and breaking encryption algorithms. There are two forms of encryption: symmetric and asymmetric. With symmetric encryption, the communicating entities share a secret (a key) that is used for encryption and decryption. With asymmetric encryption, the entities have two keys, a private key for decryption and a public key of encryption. The reverse is also true. The private key can be used to

encrypt some data. In this case, the result is a signature that can be verified by any entity having knowledge of the corresponding public key, if it knew or could compute the values of the encrypted data.

Key management systems provide the means for implementing cryptographic periods via secure distribution of new keys on a regular basis. An important point is that disclosure of the secret key during distribution could cause any cryptographic system to fail, and failing to regularly change keys could weaken the cryptographic system. Therefore, any security architecture should use a robust key management system.

Of the two approaches to key management, manual and automatic (electronic) systems, manual systems are more prone to risk because they significantly depend on human assistance, which has historically been the weakest component in any security architecture.

There are numerous flaws in both RC4 as used in WEP and in WEP itself that indicate that WEP provides no effective protection. Some examples are:

- Since 1994, researches have identified a series of flaws in RC4.
- Fluhrer and his colleagues [10] found that when RC4 is used with an initialization vector appended or preappended to the secret key, certain values of the Initialization Vector produce a weak key. An adversary who collects enough of these weak keys passively through eavesdropping can recover the secret key.
- The WEP protocol provides no form of message authentication; thus, it allows intercepted messages to be replayed or sent again without modification - see Reference [8] . While replaying packets will not permit an adversary to become a peer on the network, it can result in a significant denial-of-service attack and can be used to reduce the cost of other attacks. This lack of message authentication also permits attackers to create man-in-the-middle attacks.

C.1.2 Access control

Access control is another mechanism needed to ensure an acceptable level of confidentiality. Essentially, the purpose of access control is to allow only those who are authorized to use or view system resources. Typically, this is accomplished through an access control list (ACL), which in its simplest form is a look-up table based on some identity criteria.

Access control is strongly coupled to authentication as it relies on a valid identity (proven by authentication) to make decisions concerning access.

In theory, ACLs provide a reasonable level of security when a strong form of identity is used. Unfortunately, MAC addresses do not provide a strong identity for two reasons. First, an attacker can easily observe MAC addresses because the address must appear in the clear, even when WEP is enabled. Second, some wireless cards allow their MAC addresses to be changed via software. As a result an attacker can easily eavesdrop to determine valid MAC addresses and program the desired address into the wireless card, bypassing access control and gaining access to the network.

In most IEEE 802.11 wireless networks, the access point broadcasts the network identity using a text string call SSID (Service Set Identifier). This allows a mobile device to search for specific networks by listening to broadcasts called beacons. The idea of a closed network is to treat the network name or SSID as a secret so the mobile device must have prior knowledge of the SSID before connecting. In practice, security

mechanisms based on a shared secret are robust, provided the secrets are well protected. Unfortunately, although the SSID can be hidden in the beacon, there are several other management messages in IEEE 802.11 that contain the network name in the clear[6]. As a result, an attacker can easily sniff the network to determine the shared secret and gain access to the network. This flaw exists even with WEP-enabled networks because management frames are not protected.

C.2 Integrity

There are two aspects to integrity. With source integrity, also known as authentication, the information's originator is known and credible. With data integrity, the objective is to prevent inadvertent or malicious modification of the data.

C.2.1 Source integrity – authentication

Strong authentication requires two elements. The first is a common trust element – something or someone whom the object doing the authentication trusts and who can vouch for the entity being authenticated. The second element is unique identity for the entity being authenticated.

C.2.2 Data integrity

Ensuring data integrity requires the detection and prevention of unauthorized modifications. Whereas cryptography detects integrity violations, access control prevents integrity violations.

Access control for data integrity is similar to using access control for confidentiality; the mechanism prevents attackers from accessing and thus modifying the data. The cryptographic approach is somewhat different in that it uses a cryptographic hash function to create a unique hash value or fingerprint of the data.

Given a cryptographic hash function, detecting integrity violations is straight forward. First, compute the hash value for a given data set. Then, compute a new hash value over the same data at a later time and compare it to the previous value. If the two are not equal, the data was modified. This is done using message authentication codes and digital signatures.

C.2.2.1 Message authentication codes

Message authentication codes (MAC[7]) use a keyed one-way function to provide message authenticity proving that the contents have not been altered in route. Upon receipt, the receiver computes a MAC value over the message and compares the computed value to the received MAC. If the two values are the same, the message authenticity is valid.

While the simple MAC provides message authenticity, it should not be used in practice because a much stronger MAC exists. The HMAC MAC has a formal basis for its security properties – see Reference [7]

[6] The actual messages containing the SSID depend on the vendor of the access point.
[7] The cryptographic and security community use the acronym MAC while the IEEE uses MIC (Message integrity check). The reason the IEEE uses MIC is that the acronym MAC was already in use. This technical brochure uses MAC.

C.2.2.2 Digital signatures

Digital signatures use a cryptographic hash function such as MD5[8] or SHA1 along with public key cryptography to ensure message authentication and data integrity. To compare a digital signature, the sender first computes a hash value of the message and then encrypts this hash value using an asymmetric algorithm with the sender's private key.

The sender now sends the message and the signature to the recipient. To verify the authenticity of the message, the receiver calculates the hash value of the message and decrypts the signature using the sender's public key to obtain the original hash value. The receiver now compares the two hash values: if they are equal, the message is authentic; if they are not, the message was either tampered (data integrity attack) or not tampered while in route from the expected sender (source integrity).

C.3 Availability

Availability defines that information or resources are available when required. Most often this means that the resources are available at a rate which is fast enough for the wider system to perform its task as intended. It is certainly possible that a confidentiality and integrity are protected, but an attacker causes resources to become less available than required or not available at all. See Denial of Service discussed in Section 6.2.4.

D. The fight between WAPI and 802.11i

China's market draw for secure wireless local area networks (WLAN) technology is huge. Because WLAN manufactures want to serve a worldwide market it is important to review the competition between WAPI and 802.11. To exacerbate the situation, China at one point said that Wi-Fi chips or devices designed for use within China were going to be banned from selling in China unless they partnered with a domestic firm. With this background a brief description of the history of this competition, some insight into dirty politics, the formal vote for an international standard, and the aftermath is described.

D.1 China backs WAPI in competition with 802.11i

In the face of controversy, the Chinese government ministries have unanimously agreed to support a home-grown wireless technology as a solution to the security loophole of the existing 802.11 standard of WLAN. They claim that the technological defects of 802.11i are obvious and well known, and they note that similar concerns have been expressed by the American Nation Institute of Standards and Technology (NIST).

In May 2003, the Chinese Ministry of Information Industry (MII) declared WAPI as the national standard and said that all WLAN equipment sold in China should comply with the new technology as of December 1, 2003[9]. However, during the following annual joint commission on commerce and trade between China and the United States, China

[8] In 1996, a flaw was found with the design of MD5; while it was not a clearly fatal weakness, cryptographers began to recommend using other algorithms, such as SHA-1 (recent claims suggest that SHA-1 has been broken, however). In 2004, more serious flaws were discovered making further use of the algorithm for security purposes questionable.

[9] A transition period was granted that extended the compliance deadline for some WLAN products to June 1, 2004.

agreed to delay the enforcement of the WAPI standard because of pressure from the 802.11i camp through the American government.

D.2 Dirty politics

In other comments, some International Organization for Standardization (ISO) members also noted the intense lobbying they were subjected to during the five month balloting process. During that period, the IEEE 802.11 Working Group released detailed arguments against WAPI, which spurred angry responses from the Chinese national standards body and worsened tensions between the groups.

D.3 ISO rejects China's WLAN standard

China submitted its revamped WAPI proposal for fast track balloting, alongside 802.11i in October 2005.

The ISO overwhelmingly rejected China's domestic wireless LAN technology as an international standard, deciding instead to approve IEEE 802.11i as the basis for amore secure wireless protocol. Only 22 percent of ISO's members supported China's WAPI, while 86 percent favored 802.11i. In comments attached to their votes, some ISO members said they were concerned that WAPI's development process was relatively closed and that some of the underlying technology, such as security algorithms, has not been disclosed. There was also concern about WAPI's apparent incompatibility with 802.11i and its predecessors.

D.4 China continues the fight

Despite the rejection, this is not the end for WAPI. Many ISO members expressed a desire to see a "harmonization" between the standards. Yet it was clear that 802.11i would remain the foundation of any such attempt. Whatever happens, China has signaled its intention to keep WAPI alive[10]. China has re-ignited their campaign to establish the domestic wireless LAN technology that it claims is more secure than 802.11i.

E. IEEE 802.11i extension for management frames

The IEEE 802.11i standard patched the holes in the original WEP specification by introducing new cryptographic algorithms to protect data traveling across a wireless network. The 802.11w task group is developing extensions to protect management frames, which perform the core operations of a network.

Traditionally, management frames did not contain sensitive information and did not need protection. But with new fast handoff, radio resource measurement, discovery, and wireless network management schemes (to be provided by 802.11r, 802.11k and 802.11v), new and highly sensitive information about wireless networks is being exchanged in these non-secure frames.

- IEEE 802.11k is a proposed standard for radio resource management. It defines and exposes radio and network information to facilitate the management and maintenance of a mobile Wireless LAN. IEEE 802.11k and IEEE 802.11r are the

[10] MII predicted that China's WLAN equipment market world grow at over 30 percent to 3.59 billion yuan in 2009 (1 US dollar is about 8.03 yuan).

key industry standards now in development that will enable seamless Basic Service Set (BSS) transitions in the WLAN environment. The 802.11k standard provides information to discover the best available access point.

- IEEE 802.11r is the unapproved IEEE 802.11 standard that specifies fast BSS transitions. This will permit connectivity aboard vehicles in motion, with fast handoffs from one base station to another managed in a seamless manner. Handoffs are supported under the "a", "b" and "g" implementations, but only for data (using IEEE 802.11f or Inter-Access Point Protocol commonly known in the wireless circles as IAPP). The handover delay is too long to support applications like voice and video.
- IEEE 802.11v is the Wireless Network Management standard for the IEEE 802.11 family of standards. Task Group “v” is working on an amendment to the IEEE 802.11 standard to allow configuration of client devices while connected to IEEE 802.11 networks. The standard may include cellular-like management paradigms.
- IEEE 802.11f or Inter-Access Point Protocol is a recommendation that describes an optional extension to IEEE 802.11 that provides wireless access-point communications among multi-vendor systems.

IEEE 802.11w will extend 802.11i to cover these important frames and expects to have an official draft ratified in 2008. 802.11w will require changes to the firmware of clients and access points. It should not require hardware changes and thus might be available as a software-only upgrade to many types of hardware.

E.1 Three types of protection

802.11w provides protection in three categories. The first is for unicast management frames, or frames between one access point and one client. By reporting network topology and modifying client behavior, unprotected unicast management frames provide a powerful opportunity to an attacker. The attacker can discover the layout of the network, pinpoint the location of devices, and mount a successful denial-of-service (DoS) attack.

802.11w extends the existing notation of data encryption algorithms to the unicast management frames, using the existing Temporal Key Integrity Protocol or Advanced Encryption Standard (AES)-based algorithms. This protects against forgeries and provides confidentiality.

The second method is for generic broadcast management frames. These frames are less common and typically are used to adjust radio frequency properties or start of measurements, rather than report sensitive information. Thus, 802.11w protects only against forgeries, and does not provide confidentiality. The simplest proposal under consideration relies on a message integrity code, which is appended to the non-secure management frame. An access point shares a key with every securely associated client. All devices, including eavesdroppers, can see the message, but the key prevents devices outside the network from forging messages. However, the authenticated clients can still pretend to be the access point in this scheme.

The third method is for deauthentication and disassociation frames. By using a pair of related one-time keys, one secret in an access point and one for a client, the client can determine if the deauthentication is valid. This method can present problems for users who deploy or are considering intrusion-prevention systems in their networks.

By protecting the contents of most management frames from eavesdropping, and of certain crucial frames from forging, 802.11w will stop the information leakage and reduce some basic DoS attacks.

E.2 How 802.11w works

Figure 21 shows one example of how an access point and clients are setup to use 802.11w management frames and exchange all necessary keys.

1. The access point sends a unicast 802.11k measurement request. The sensitive results of this measurement are sent back by the client. In both cases, the contents of the messages are hidden from the attacker.
2. The attacker tries to send a forged measurement request. But because the attacker doesn't know the key, it can't properly encrypt the measurement request, and the client drops it without harm.
3. The access point uses message integrity code to send a broadcast frame to the clients to adjust their power. The clients verify the message with the integrity key. The attacker also sees the messages and knows the contents but can not forge a new message from it.
4. The attacker tries to broadcast a deauthentication message. The clients receive the message and compare their one-time keys to the one in the message. Because the attacker doesn't know the one-time key of the access point, the keys won't match, and the clients safely ignore the message.

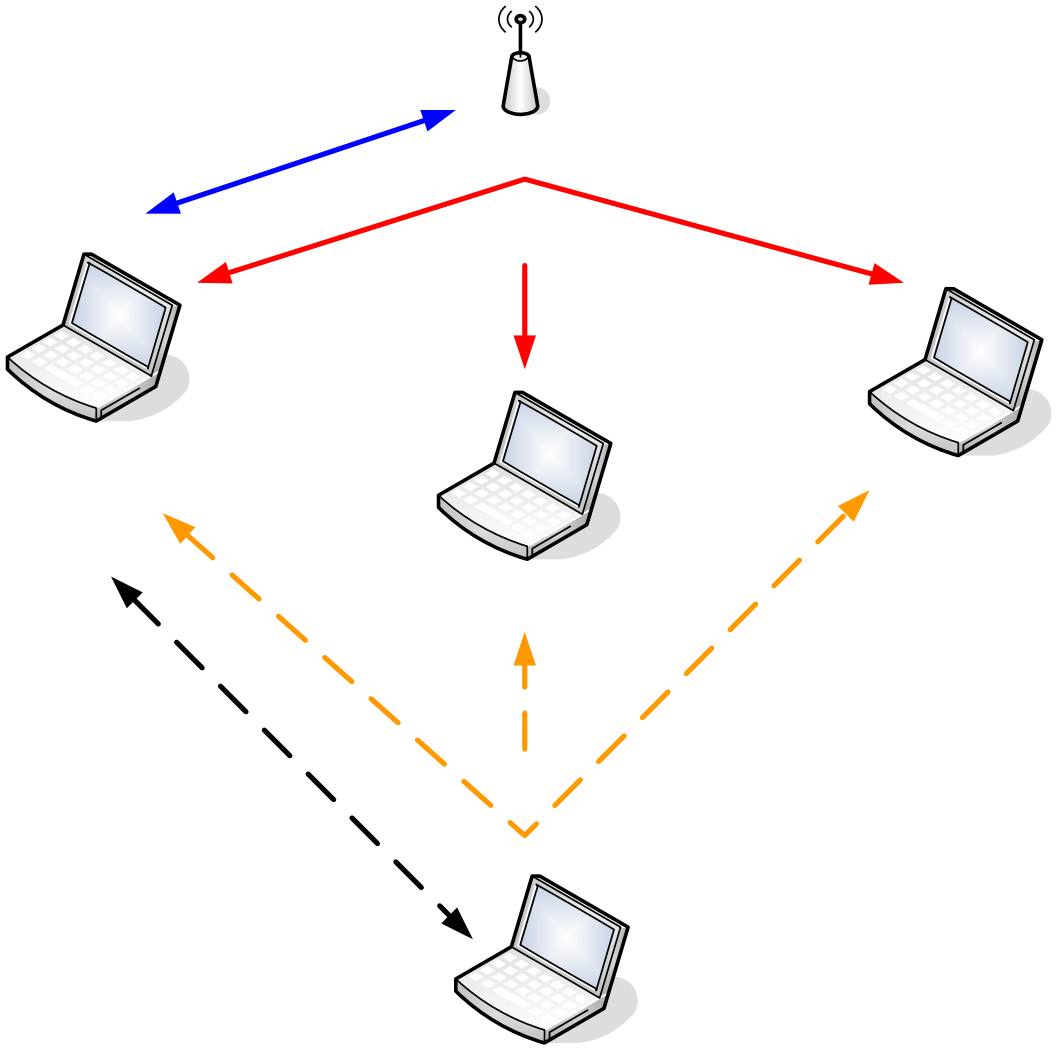

Figure 21 How IEEE 802.11w works

F. Radio planning for Wi-Fi coverage options

One of the requirements for a Wi-Fi network deployment is to define its coverage area. Though it may seem quite obvious, a security requirement can also be imposed in the physical layer; i.e., **be sure that you only provide coverage in the requested area**. To establish a customized coverage area, a specific type of antenna is required.

In certain installations, it will be desirable to change the omni-directional antenna gain pattern to a more complex one. There are several antenna types available in the market such as sector panel antennas, directive antennas, and patch panel antennas. All these antennas are characterized by their antenna gain pattern.

Figure 22 depicts an ideal omni-directional antenna gain pattern taken from vendor data sheets. The azimuth (or horizontal) beam width is 360º. The elevation (or vertical) beamwidth is of 28º.

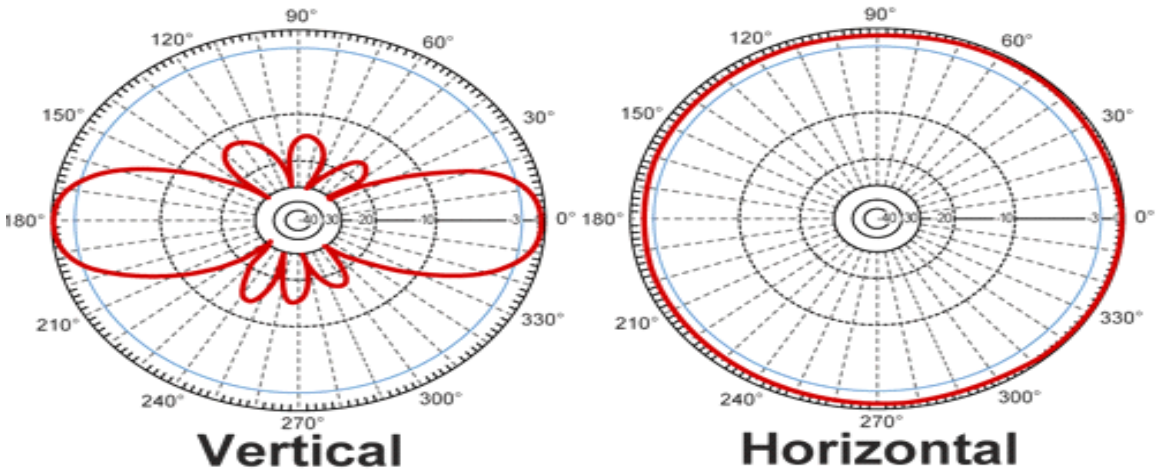

Figure 22 Omni-direction antenna gain pattern

First, let's compare above antenna gain pattern with a sector panel antenna gain pattern. Though they have a similar elevation (vertical) beam width, the azimuth (horizontal) beam width shown in Figure 23 is quite different. The sector panel antenna azimuth (horizontal) beam width is of 90º. Clearly, the sector panel antenna is a better choice to cover a square area such as when the Wi-Fi access point is installed in one corner of the substation fence.

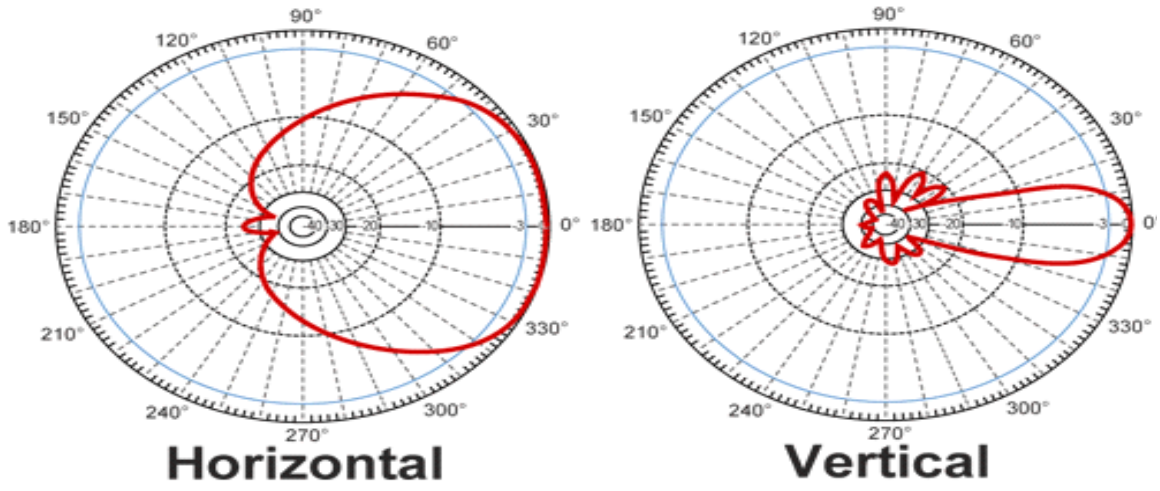

Figure 23 Sector panel antenna gain pattern

In this appendix we have only mentioned the antennas, as the key part to provide Wi-Fi coverage to a certain geographical area. There is other radio equipment that may be useful such as power amplifiers, which increase the transmitted signal power and amplify the received signal level. Splitters are also an interesting device that allows a single Wi-Fi access point to serve different coverage areas. Finally, we cannot forget

mentioning the antenna cables. We may have designed a radio link using an appropriate antenna and selecting a very good power amplifier, but unless the antenna cable characteristics are taken into consideration, the radio link design will not have the required performance.

It should also be noted that when planning a Wi-Fi coverage area, performance and RF channel assignment should be considered.

- Required performance. Include both the maximum throughput and the number of network users. The maximum throughput is limited by the received signal strength as compared to the noise level. Also, as the number of users to be served increase, the number of Wi-Fi access points must be increased.
- RF channel assignment. For example, though in IEEE 802.11b there are 14 different RF channels available, when planning a coverage area, the network planner will only use three different RF channels (Channels 1, 6, and11). In this way, all channels are separated as much as possible to avoid possible interferences.

G. Countries participating in CIGRE survey

Argentina	Denmark	Ireland	Portugal
Australia	Ecuador	Israel	South Africa
Austria	El Salvador	Italy	Spain
Belgium	Finland	Lichtenstein	Sweden
Canada	France	Malaysia	Thailand
China	Germany	New Zealand	United Arab Republic
Cypress	Greece	Nigeria	United Kingdom
Czech Republic	Indonesia	Philippians	United States

H. Approaches used to reduce vulnerability on transmission and distribution operational networks

The Wi-Fi survey results summarized in Chapter 3 produced some surprising results. Another related study (see Reference [19]) was used by the working group to gain more insight into the approaches used to reduce vulnerability on transmission and distribution operational networks. Reference [19] is important because it updates a 2003 survey and reflects the opinion of operations management and senior staff from 245 utilities and more than 30 countries. The results of these surveys to reduce cyber vulnerabilities by the end of 2005 are summarized for both North America and International respondents.

H.1 North American utilities

Figure 24 summarizes the results of a survey of North American utilities to reduce cyber vulnerabilities.

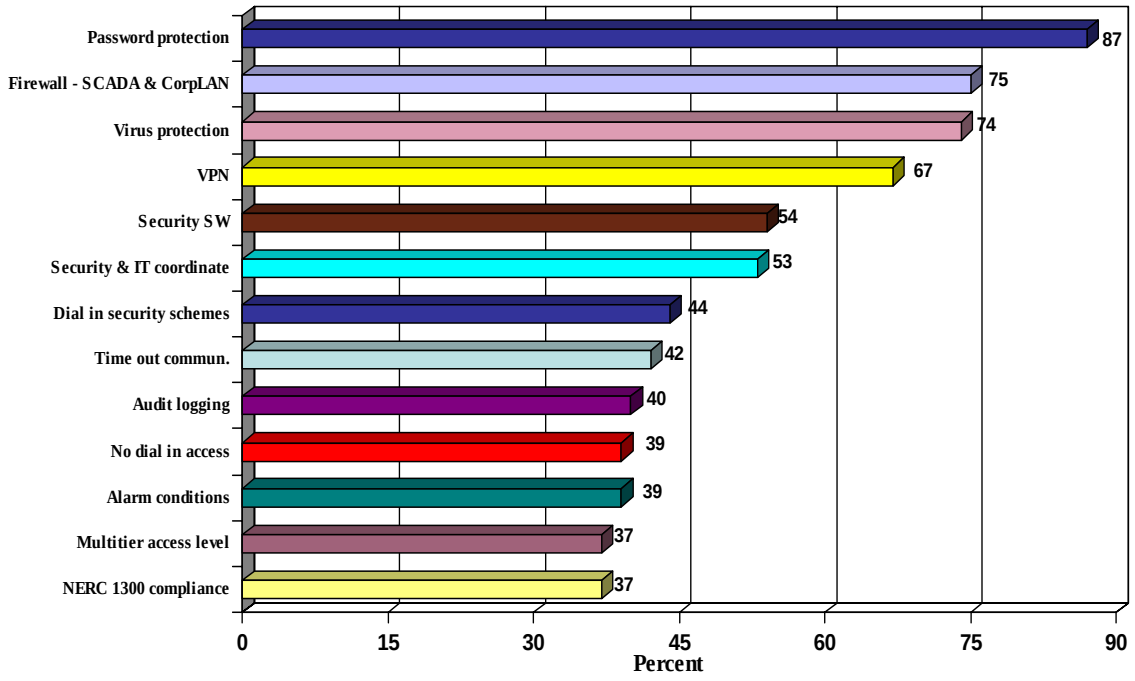

Figure 24 Current and planned use by North American utilities to reduce cyber vulnerabilities

This group of 147 respondents cited password protection as the most frequently used approach (87%) to reduce vulnerability on operations networks. Unfortunately, a dedicated and trained intruder most likely can crack many password schemes in use at utilities within hours. Firewalls had by mid-2005 been established between the control center systems and other utility IT systems in 75% of the utilities replying to this question, up significantly from the 2003 study. These results further reinforce the need to provide strong access control and use control mechanisms as offered by IEEE 802.11i and ANSI X9.69 standards.

Virus protection software was being used by 74% of the group. Another approach that has increased significantly from the 2003 study is the use of virtual private networks (or VPNs). While the 2003 study found 45% using VPNs, the percentage has risen to 67% in the current study.

Cooperation between IT and operations is improving rapidly. More than one half of the respondents indicated that use of security software packages and security efforts are now being coordinated with enterprise IT efforts. This cooperation is needed to ensure a comprehensive solution throughout the enterprise and avoid stove pipe solutions invented by one particular organization.

The continuing good news can be found in the increased use of multiple cyber security approaches being adopted by North America's electric utilities. The largest utilities, investor-owned, other public power utilities, and Canadian utilities were likely to use more approaches for reducing vulnerability on their operational networks than were the municipals and cooperatives.

At least one-half of the utilities serving at least 250,000 customers were likely to have implemented 12 of the listed vulnerability reduction measures, a significant increase over the findings reported in the mid-2003 study.

The good news extends to the finding that utilities serving fewer than 100,000 customers are using multiple approaches as well, from basic vulnerability reduction tools such as password and virus protection on up to some encryption, audit logging and substantial use of VPN techniques.

Investor-owned utility officials were making use of all but a few defense approaches at a much higher rate than were the subgroup's counterparts in public utilities, cooperatives, and among the Canadian group of utility officials.

H.2 International utilities

Figure 25 summarizes the results of a survey of International utilities to reduce cyber vulnerabilities.

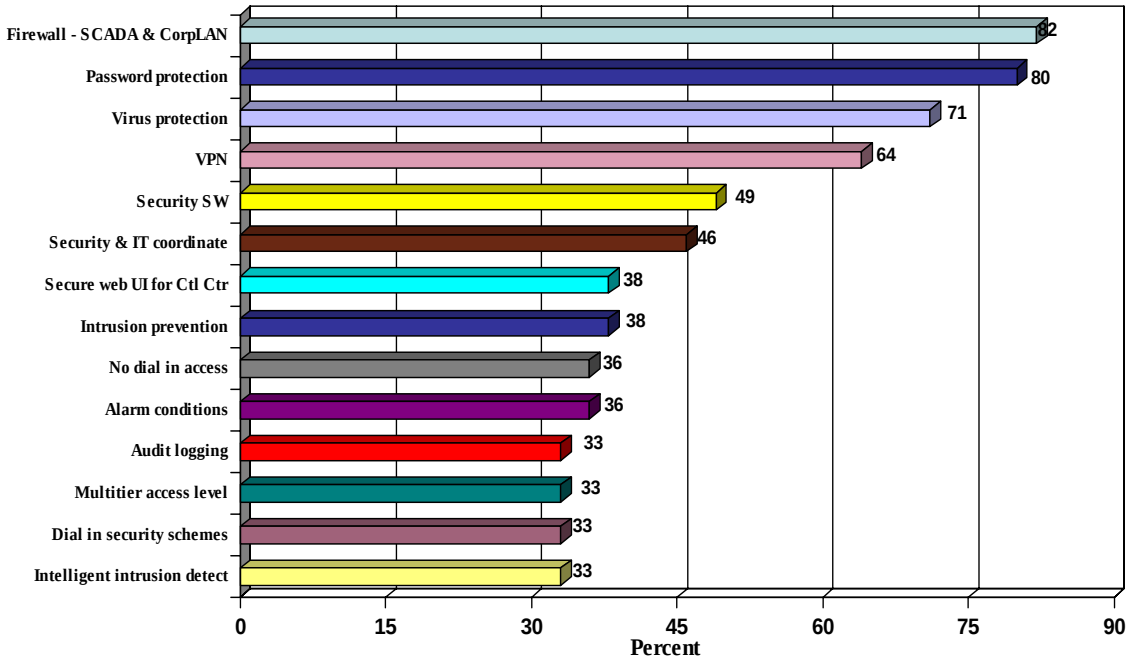

Figure 25 Current and planned use by International utilities to reduce cyber vulnerabilities

In this study 55 utility officials shared information regarding use and plans for using methods to reduce vulnerability on operational utility networks. A total of 22 methods and techniques were listed on the survey. The most important measures being used or planned included: firewalls between SCADA/DMS and the corporate LAN; password protection, followed by virus protection, VPN use and security software.

Some regional variances were observed. European officials concurred with the top five approaches listed above. Asia-Pacific officials mentioned VPNs and firewalls slightly

above passwords and virus protection. The rest-of-world regions ranked password protection first, then firewalls, virus protection, security software and VPN use.

Importantly, on average international utilities had adopted eight of these vulnerability reduction measures, a very significant improvement over the 2003 study.