



Resilient Wireless Data Communication for Critical Infrastructure

**Securing wireless data communication for
mission critical applications**

A White Paper by

Matthias H. van Doorn

Product Manager, Ethernet & Licensed Spectrum Radio Systems

FreeWave Technologies, Inc.

July, 2010

Resilient wireless data communication for critical infrastructure

Copyright © 2010 FreeWave Technologies, Inc.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior permission of the copyright owners.

Resilient Wireless Data Communication for Critical Infrastructure

Document No.:

Published by FreeWave Technologies, Inc., July 2010

Any comments relating to the material contained in this document may be submitted to:

FreeWave Technologies, Inc.
1880 S. Flatirons Ct., Suite F
Boulder, CO 80301-2850
USA

or by email to:

moreinfo@FreeWave.com

Table of Contents

Executive Summary	4
Critical Infrastructure	5
Cyberspace	6
Security Threats	7
Denial of Service	7
Intrusion	7
Wireless Data Communication	8
Wireless Resiliency	9
Frequency Hopping Spread Spectrum	9
Access Control	10
Authentication, Authorization and Accounting	10
Privacy	11
Encryption	11
Policies	11
Limitation of permitted activities	11
Convenience	12
Conclusions	13
About the Author	14
About FreeWave Technologies, Inc.	14



*Securing wireless data communication
for mission critical applications*

Executive Summary

Vital public services – Utilities, Transportation, Manufacturing, Trade, Finance, Service Industries, Public Safety and National Defense – are now all dependent on computer systems connected through data communication networks and the integrity, confidentiality, and availability of the data they contain. As cyberspace evolves, it is becoming more attractive and more vulnerable to exploitation and attacks, seeking to steal, corrupt, harm or destroy.

This white paper discusses some of the security threats and options to make wireless data communication networks for critical infrastructure applications more resilient and secure. It explains rugged wireless transmission systems, access control through authentication and authorization, data privacy through encryption and other security strategies. The concepts will be of interest for both IT managers or IT personnel, as well as engineers or technicians responsible for wireless connectivity, automation or SCADA systems and may provide ideas on how to improve existing or new wireless data communication networks.

Vital public services – Utilities, Transportation, Manufacturing, Trade, Finance, Service Industries, Public Safety, National Defense – are now all dependent on computer systems connected through data communication networks and the integrity, confidentiality, and availability of the data they contain.

Critical Infrastructure

If you think about critical infrastructure, the things that come to mind are all of the services and assets that make civilized life possible. Those include

- our Water Supply; drinking water but also waste water and sewage
- Heating (e.g. natural gas, heating oil or other fossil fuels like coal)
- Electricity (generation, transmission, distribution, consumption)
- Telecommunication
- Oil and gas as fuels or for chemical production (oil and gas products production, transport, refineries, distribution)
- Transportation systems (roadways and bridges, railways, airports, harbors, inland shipping etc.)

as well as financial services (banking); public health services (hospitals, ambulances) or public safety and security (police, fire, military) and others.

All of these are critical to our daily lives and essential for the functioning of our society and economy¹.



Photo 1: Pump Jack, San Juan Basin, New Mexico

¹ According to the "Presidential Decision Directive 63" (PDD-63) from May 22, 1998: "critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government."

Cyberspace

SCADA

SCADA, short for Supervisory Control And Data Acquisition, generally refers to a control system which consists of a computer or system monitoring and controlling a process.

- *Industrial processes include those of power generation, fabrication, manufacturing, production and refining etc.*
 - *Infrastructure processes include water treatment and distribution, wastewater collection and treatment, oil and gas pipelines, electrical power transmission and distribution etc.*
 - *Facility processes occur in buildings, airports, ships, and space stations and can monitor and control HVAC, access, energy consumption.*
-

With the introduction of computer technology, the proliferation of networks that enabled data exchange between computers and the birth of the Internet, mankind saw the dawn of a new, virtual environment aptly named “cyberspace”.

The way the implementation of technology and cyberspace not only reshaped our daily activities but also our social interactions, has been revolutionary. In fact, the impact of cyberspace altered most parts of our lives ranging from the way we do business, get information and knowledge about health issues and select health care providers, to the way we get the news or receive our entertainment (music or movies) or share our interests and knowledge about subject matters.

These days, we can look at our electric bill on-line and make the payments on-line, rather than using physical paper and the good old US Postal Service. The evolution of Smart Grid Technology even promises us to have real-time access to data that shows us how much electricity we are using this very minute and at what cost, thereby giving us the opportunity to influence our consumer behavior (and reduce our bill in the process). All of this is made possible by automation and data communication systems (like modern SCADA systems) that enable the integration of command and control functions for critical infrastructure into cyberspace.

But as cyberspace evolves, it is also becoming more attractive and more vulnerable to exploitation and attacks, seeking to steal, corrupt, harm or destroy. In fact, the actual threat of hackers attacking critical infrastructure from communication networks to financial institutions or even the electric grid has become very real.

Attacks on critical infrastructure themselves are nothing new; back in World War II for example, the electric grid in Germany was the target of bombing raids aiming to disrupt factories and industrial production by interrupting or completely denying the much needed supply of electricity.

These days, America’s enemies could exploit our very own cyberspace security vulnerabilities to interrupt our critical infrastructure such as the electric grid, as acknowledged by both the Pentagon and the Department of Homeland Security. In fact, military officials now describe cyberspace as the fifth domain of war (following land, sea, air, and space) and note that cyberspace is unique, as it is the only battlefield to be invented by humans.

With threats to our information infrastructure and data communication networks (including wireless SCADA networks responsible for critical infrastructure) increasing in both frequency and sophistication and many recent examples of attacks and the impact on their targets, it is no wonder that many organizations and even branches of the government are now looking at addressing the issue with new policies and security standards².

² See “[The National Strategy to secure Cyberspace](#)”, The Department of Homeland Security, February 2003

Resilient wireless data communication for critical infrastructure

The *Cybersecurity Enhancement Act of 2010*, H.R. 4061 or the grant for a National Electric Sector Cyber Security Organization for Cybersecurity for Energy Delivery Systems, funded by the NETL and the US Department of Energy (DoE) are other good and more recent examples.

Security Threats

The two most common threats to data communication networks today are *Denial of Service (DoS) Attacks* and *Network Intrusion*.

The National Security Agency (NSA) is currently launching a new program to monitor government and critical infrastructure networks for signs of cyber attack”

July 2010

Denial of Service

An attempt to make a computer resource or network unavailable to its intended users, Denial of Service could be as simple as jamming an electric or electromagnetic signal or as sophisticated as saturating a system or network with communication and data traffic intended to overwhelm and avoid legitimate data to get through and be processed. Consequences of Denial of Service attacks range from being simply irritating, for example when services are unavailable or slow to respond, to dire, when critical control signals don't reach the intended destination and for example a valve does not open to provide coolant liquid to a system threatening to overheat or a pump that does not turn on as intended to reduce fluid levels threatening to flood an area.

Intrusion

Penetrating and intruding into a network or computer resource is a different story and level of sophistication. Consequences can range from passive attacks (eavesdropping) and simply spying out or stealing information to corrupting data or maliciously, intentionally causing harm or destruction by taking over network and/or computers and control systems. For example, intentionally opening valves or controlling pumps in a wastewater system resulting in contamination or pollution or remotely opening pressure valves on a pipeline, allowing oil or gas to escape into the environment.

By no means is this a complete list of threats and potential attacks, after all, there are for example many published cases of disgruntled employees (or former employees) causing all sorts of security breaches and havoc.

Sophisticated command and control attacks, packet spoofing, hijacking of sessions, replay attacks, the use of worms, Trojans and remote controllable Trojans (Back Orifice), the use of a Virus and Anti-forensic techniques as well as attacks on DNS infrastructure are not limited to wireless networks and need to get addressed as part of an overall IT security strategy.

Wireless Data Communication

“I do not think that the wireless waves I have discovered will have any practical application”

Heinrich Rudolf Hertz

Unlike traditional wire-line data communication, which typically uses copper or fiber-optic cable between communication endpoints, wireless data communication is based on electromagnetic waves using radio frequencies (RF) propagating through open space, literally the air. This gives wireless some unique advantages, as communication endpoints don't need to be tied down to a fixed location and access to a physical cable. In addition, running cable, conduit or even digging trenches between communication endpoints can be a time-consuming, expensive and sometimes even potentially dangerous proposition.

The Flexibility of wireless data communication however comes at a price. Electromagnetic waves are non-discriminatory when it comes to access; while a wired connection requires physical access to the cable, wireless connections can be made anywhere along the path on which the electromagnetic waves propagate. You can't make radio waves stop at the edge of your property with a simple split-rail fence; the physics are a little more complicated than that.

Consequently, security (as in secure access) becomes much more important for wireless data communication.

Case and point, who has not heard a story of a guy in the parking lot that hacked a Wi-Fi connection to steal Internet access or gain access to private data (like credit card or bank information) through an unprotected wireless network? A case that actually made the news was that of a 21-year-old Michigan man who attempted to steal credit card numbers from a Lowe's home improvement store through their unsecured Wi-Fi network from inside his vehicle in the store's parking lot back in 2004 and who was sentenced to 9 year in prison after he was caught³.

And who did not wish the movie theatre or church did use a cell phone jamming device (even though their usage isn't legal in our country) when listening to the ring tone of a cell phone or worse, annoying phone calls in the middle of a movie or sermon, in order to suppress those pesky wireless cell phone calls by people oblivious to their environment?

Besides thwarting attempts of insurgents to remotely and wirelessly detonate improvised explosive devices, those foreign made jamming devices are perfectly suitable to keeping the peace not just on foreign battlefields.

³ For more information on the specific case, see <http://www.securityfocus.com/news/10138>

Wireless Resiliency

“An object of the invention is to provide a method of secret communication which is relatively simple and reliable in operation, but at the same time is difficult to discover or decipher.”

*Hedy Kiesler Markey and
George Antheil, June 1941*

US Patent Serial No. 397,412

It was back in 1941 when Hedy Lamarr, an Austria born actress, together with George Antheil co-patented a “*secret communication system*” which allowed radio control of torpedoes that could not be easily discovered, deciphered or jammed⁴.

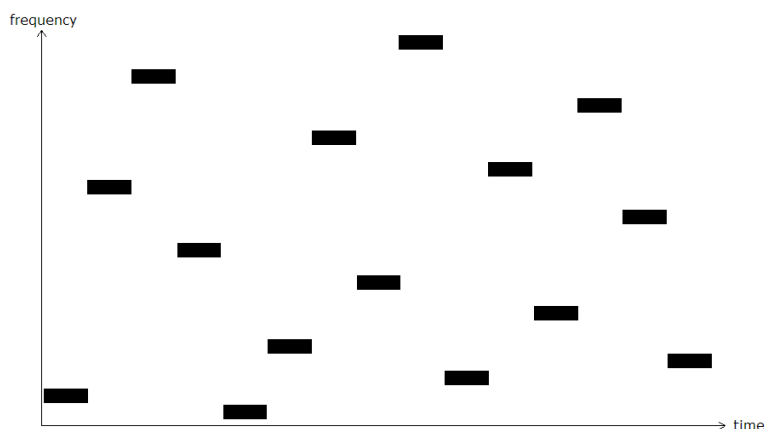
Her secret: **Frequency Hopping!**

Coordinated, rapid changes in radio frequencies would literally “hop” in the radio spectrum, thus evading detection and the potential of interference, in other words, being suppressed or jammed.

Even though her idea was ahead of its time and not implemented in the USA until 1962, when it was used by U.S. military ships during a blockade of Cuba (after the patent had expired), it is the basis for modern Frequency Hopping Spread Spectrum (FHSS) wireless communication systems.

Frequency Hopping Spread Spectrum

Frequency Hopping Spread Spectrum (FHSS) wireless systems are very resilient when it comes to impairments such as interference (deliberate or coincidental) and “jamming” or other effects that can be observed when wireless signals travel through space, such as the “multipath” phenomenon, simply because they use only very small amounts of radio spectrum at a time and don’t dwell (or remain) at that frequency long, instead “hop” to another frequency quickly. Statistically, chances are that the signal does not “land” at the interfering frequency, thereby successfully evading the jamming signal. This makes a Denial of Service (DoS) attacks on FHSS systems very difficult, albeit not completely impossible.



Graphic 1: Frequency Hopping

A resilient wireless system however needs more than just a rugged transmission system like FHSS.

⁴ [Copy of the US Patent 397,412 by Hedy Lamarr and George Antheil](#)

Access Control

In computer security, access control includes authentication, authorization and accounting (e.g. logging access and activities for security audits)

There are many positive things that can be said about “industry standard” based wireless devices. One of the negatives about them is the fact that all that is required to connect is an “off the shelf”, standard based device compatible with the ones used in a specific wireless network to gain access to it. Case and point; a Wi-Fi card for less than \$50 is all I would need to try to gain access to the electromagnetic waves emitted by my neighbors Wi-Fi Access Point and his Internet connection. And if he did not protect it, that’s all I need to get “free” Internet access through his Wi-Fi network.

Proprietary systems and devices, especially when they offer many “knobs” and configuration options to create more private networks, actually offer a higher degree of security. But even those devices can be acquired if you know where to get them (a well known Internet auction place often serves as the source) so that a patient hacker can figure out settings to gain access, even if it may take a while.

Therefore, Access Control is one of the most important security features to prevent unauthorized access and intrusion.

Authentication, Authorization and Accounting

The cyberspace equivalent of the security guard at the main door of an office building that makes sure only people with the correct badge can enter, the goal of access control is to only allow network access by authorized devices and to disallow access to all others. Access should be authorized and provided only to devices whose identity has been established (authenticated) and whose placement on the network is approved in accordance with network plans, designs or policy.

The verification of identity, or *Authentication*, is based on the presentation of unique credentials to that system. The unique serial number of a wireless device for example (that hopefully can neither be “spoofed” nor counterfeited) may be such a unique credential.

Remote Authentication Dial In User Service (aka "*RADIUS*") is a popular method to provide centralized Authentication, Authorization, and Accounting (“AAA”) to manage access to wireless networks.

In 1973, Horst Feistel, a Berlin (Germany) born Physicist, published an article with the title 'Cryptography and Computer Privacy' in a magazine called 'Scientific American', in which he tried to cover the most important aspects of machine encryption and introduced what became the basis of the Data Encryption Standard (DES) in 1977.

Privacy

A good network security strategy should go even further and protect data “in transit” as well, so that even a device that managed to gain access to the network doesn’t necessarily gain access to the actual data without passing yet another layer of security.

For thousands of years, cryptography provided this extra layer and maintained the privacy of the actual data between the sender and recipient, even if others had access during transit or transmission.

Encryption

Methods of encryption and deciphering have come a long way since the days of Pharaohs in old Egypt. Today, the Advanced Encryption Standard (AES) is “the” industry standard for encryption. No wonder, considering that its roots go back to the National Institute for Standards and Testing (NIST) acting on the need for a new encryption algorithm capable of protecting top secret information. A Federal Government standard and even used by the NSA, it can be trusted to protect sensitive information and maintain data privacy.

Security Policies

The aforementioned are only a few basic features that can help with creating a resilient wireless data communication system for critical infrastructure.

A good network security strategy however needs to address and implement policies as well that serve as safeguards, making it difficult to circumvent security measures and limit the potential impact of a security breach of the wireless network. Consider those added layers of security.

Limitation of permitted activities

One method to implement safeguards is to limit permitted activities on the wireless network to only those absolutely required on the network. The basic idea is that if a wireless network were to be compromised, the impact would be limited. In other words, a wireless network primarily used for sensor data collection and remote control of devices should not allow a hacker that compromised the network to gain access to financial or other critical data.

Such a limitation of permitted activities can be achieved through:

1. **Firewalls and Packet Filters**; these essentially separate the information needed on the wireless network from that available on other parts of the network.

Resilient wireless data communication for critical infrastructure

2. **Virtual LAN's** (VLAN's or Virtual Local Area Networks); separating the wireless network infrastructure and its management from the production network and devices or communication endpoints by using virtual LAN's introduces another level of security, especially if combined with Quality of Service (QoS) mechanisms. Think of it as an emergency access to your wireless network infrastructure for remote management and control in case a Denial of Service (DoS) attack overwhelms the actual payload and production network.
3. **User Level Access**; by implementing user level access (password protected), you can provide access to your wireless infrastructure and devices to e.g. maintenance personnel, but limited to monitoring system health or performance without opening the system up to misuse or sabotage because configuration and other privileges are reserved for a different user level and password.
4. **Access limitation of local ports**; by controlling who is allowed access from local ports (e.g. through MAC address filtering) or even completely turning off local port access when they are not in use, you can essentially make it impossible (or at least very hard) for someone who gained physical access to your network infrastructure and devices to get connected and gain access to your network.
5. **Audit Logs**; not really limiting permitted activities, activity logs do provide a trail of access and activities and can be a useful tool in auditing and tracing potential security breaches and issues.

Again, this is by no means a complete list of options to secure a data communication network. It does however provide a good baseline and you should consider if your wireless data communication equipment and devices support these advanced features and even Secure Shell (SSH) for their own configuration menus or really only provide basic connectivity, especially when they are being used for critical infrastructure applications. Vendors like FreeWave Technologies, Inc. take wireless security seriously and offer devices that support these features.

Convenience

Often, convenience is the main reason behind opening Firewalls, giving users too many privileges and too much access or even worse, using default settings and passwords (or not changing these passwords regularly, not requiring complex passwords or a minimum password length) that render other protective measures useless and are violating any cybersecurity best practices. This presents a major cyber vulnerability and imminent threat to critical infrastructure, where disruptions could result in catastrophic damage up to loss of life and property.

Security should come first and not be treated as an afterthought. And security should never be compromised for convenience.

In Conclusion

Any chain is only as strong as its weakest link and we need to start building and implementing adequate protections for our wireless data communication networks for critical infrastructure with the goal to make them more resilient, malicious hackers will keep exploiting, attacking and ultimately, destroying.

About the Author

Matthias H. van Doorn is the Product Manager for Ethernet and licensed radio systems at FreeWave Technologies Inc.

He has more than 15 years of experience in the telecommunications industry and has previously worked for companies such as CalAmp Corp., ADC Telecommunications, Digi International and Siemens.

Mr. van Doorn holds a B.Sc. degree in electrical engineering and an MBA in international business.

About FreeWave Technologies, Inc.

Renowned for unparalleled performance, reliability and durability in even the harshest of conditions, FreeWave spread spectrum and licensed radios remain the trusted choice of military, government, industrial and municipal customers who depend on “*Communication Without Barriers*”.

Founded in 1993 and privately held, FreeWave blends unsurpassed technical product knowledge and customer support - *FreeWave Rapid Response*, with comprehensive engineering to provide complete solutions for diverse industries such as oil and gas, military, utilities, security and recreation.

Because of FreeWave’s unwavering commitment to quality and customer service, FreeWave is the only company of its kind to offer rigorously tested radios that are 100 percent backward-compatible and backed by a 2-year warranty.

Contact FreeWave today at 303.381.9200 or moreinfo@FreeWave.com to learn more about how our practical, cost-effective solutions can meet your precise communication needs.