

# **Resilient Wireless Data Communication for Critical Infrastructure**

By Matthias H. van Doorn, FreeWave Technologies, Inc.

## Critical Infrastructure

When you think about critical infrastructure, what comes to mind are all of the services and assets that make civilized life possible. It includes: our water supply (drinking water, waste water and sewage); heating (e.g. natural gas or heating oil); electricity (from generation, transmission and distribution to our 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.); financial services (banking); public health services (hospitals, ambulances) or public safety and security (police, fire, military) and many others.

These components of our infrastructure are critical to our daily lifestyles and essential for the efficient functioning of our society and economy.

## Cyberspace

With the introduction of computer technology, the proliferation of networks has enabled data exchange between computers and given birth to the Internet. Now, mankind is experiencing the dawn of a new, virtual environment aptly named "cyberspace."

The implementation of new technology and cyberspace not only has reshaped our daily activities, but has revolutionized our social interactions. In fact, the impact of cyberspace on our lives has been staggering. From the way we do business, to gathering information and knowledge about health issues, to the way we get the news or receive our entertainment (music or movies) or how we share our interests and knowledge about subject matters within online communities.

These days, we can review and pay our electric bills online, rather than using physical paper and the good-old U.S. Postal Service. The evolution of Smart Grid Technology even promises to have real-time access to data that shows how much electricity we are using this very

minute, and at what cost, thereby giving us the opportunity to influence our consumer behaviors (and reduce our bill in the process).

All of this is made possible by automation and data communication systems that have enabled the integration of critical infrastructure into cyberspace.

However, the evolution of cyberspace has made it more attractive and more vulnerable to exploitation. There has been an increase in attacks, stealing, corruption, harm and destruction to our systems. 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. For example, back in World War II, the electric grid in Germany was the target of bombing raids aimed at disrupting 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 disrupt 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, it is no wonder that many organizations, and even branches of the government, are looking at addressing the issue with new policies and security standards.

The grant for a National Electric Sector Cyber Security Organization for Cybersecurity for Energy Delivery Systems, funded by the NETL / the U.S. Department of Energy (DoE) is a good example (see at <http://www.netl.doe.gov> ) or the Cybersecurity Enhancement Act of 2010, H.R. 4061 ([http://www.rules.house.gov/111/LegText/111\\_hr4061\\_txt.pdf](http://www.rules.house.gov/111/LegText/111_hr4061_txt.pdf) )

The Threats

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

Denial of Service is 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. The consequences of DoS attacks can range from being simply irritating, for example, when services are unavailable or slow to respond – to dire – such as when critical control signals don't reach the intended destination. 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.

Penetrating and intruding into a network or computer resource requires a different level of sophistication. Consequences can range from simply spying or stealing information to corrupting data or maliciously and 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 many published cases of disgruntled employees causing all sorts of security breaches and havoc in the workplace.

### Wireless Data Communication

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 dependent upon a physical cable. In addition, running cable, conduit or even digging trenches between communication endpoints can be a time-consuming, expensive and sometimes even a potentially dangerous proposition.



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

FHSS wireless systems are very resilient when it comes to impairments such as interference (deliberate or coincidental) and "jamming." Other effects 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.

This makes a Denial of Service (DoS) attacks on FHSS systems very difficult, albeit, if not completely impossible.

However, a resilient wireless system needs more than a rugged transmission system.

### Access Control

There are many positive attributes of "industry standards" based wireless devices. However, one of the negative aspects is that the only requirement to connect this wireless device is an "off-the-shelf," standards-based device -- compatible with the ones used in a specific wireless network -- for access.

Case and point: a less than \$50 Wi-Fi card is all I would need to try to gain access to the electromagnetic waves emitted by my neighbor's Wi-Fi Access Point and 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.

It is the 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.

## Privacy

A good network security strategy should go even further and protect data "in transit" as well. Even if an unauthorized device manages to gain access to the network, it 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.

Methods of encryption and deciphering have come a long way since then. 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. As a Federal Government standard, and even used by the NSA, it can be trusted to protect sensitive information and maintain data privacy.

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

Other tools that can help "harden" a wireless data communication network may include policies to limit permitted activities to the minimum required for business purposes, such as User Level Access and Filtering (MAC addresses or IP packets). Often, convenience is the

reason behind opening Firewalls, giving users too many privileges and too much access, or, even worse, using default settings and passwords that render other protective measures useless, thereby violating many cyber-security best practices. This presents a major cyber vulnerability and an imminent threat to critical infrastructure where disruptions could result in catastrophic damage up to loss of life and property.

Any chain is only as strong as its weakest link. If we don't start building and properly implementing adequate protections for our wireless data communication networks, (especially for our critical infrastructure, with the goal of making them more resilient) malicious hackers will keep exploiting, attacking and ultimately destroying our way of life.

-----  
About the Author

Matthias van Doorn is the Product Manager for Ethernet and licensed radio systems at FreeWave Technologies Inc. [\(insert special link\)](#)

He has more than 15 years experience in the telecommunications industry and previously has 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.