WIRELESS TECHNOLOGIES AND THEIR APPLICATION TO NUCLEAR POWER PLANTS

Brian Kaldenbach and Michael Moore*
Oak Ridge National Laboratory
P.O. Box 2008, MS-6075
Oak Ridge, TN 37831-6075
E-mail: kaldenbachbj@ornl.gov and mooremr@ornl.gov

Wayne Manges
Oak Ridge National Laboratory
P.O. Box 2008, MS-6006*
Oak Ridge, TN 37831-6006
E-mail: mangesww@ornl.gov

Keywords: Wireless, Wireless LAN, RFID

ABSTRACT

Wireless technologies have matured to the point of standardization and wide acceptance in industry and at home. In fact, the increased use of wireless in the past few years has been explosive. With such wide acceptance outside of nuclear power plants, one must expect that these technologies in time will impact the environment of all industrial plants, including nuclear power plants. However, the convenience of this technology comes with a cost; specifically, electromagnetic interference upsets and surreptitious “attacks” from over-the-air are issues that must be dealt with properly for use of wireless technologies to be effective. To complicate matters, the definition of wireless is not straightforward to the user community. The term “wireless” includes devices such as cell phones, radiofrequency identification (RFID) tags, and wireless local area network (WLAN) devices.

This report provides a survey and analysis of available wireless technologies, primarily focusing on WLANs, and it includes issues of deploying them in a nuclear power plant. The analysis will include the current maturity level of wireless technologies and a discussion of the general intercompatibility of the various technologies. This will encompass protocols, bandwidths, and drivers, as well as potential for harm. Interference with other electronic systems and potential security breaches will be addressed specifically.

This paper will help future instrumentation and controls designers select compatible wireless systems for nuclear plants. It will also result in recommendations for administrative controls that plant operators may need to put in place should wireless systems be deployed.
1. INTRODUCTION

Every once in a while, a new technology becomes available that has a huge impact on how we conduct business or operations. The standardization of wireless local area network (LAN) technology has allowed such an impact. Inexpensive products have flooded the marketplace that provide a good level of performance and provide untethered access to computing resources in the workplace and at home. One can easily argue the increase in productivity that is possible by providing users of computing resources with wire-free capabilities. However, convenience almost always comes with a cost, and wireless access is no exception. Another wireless technology that has the potential to transform operations in industrial environments is radio frequency identification (RFID) tagging. Small RFID devices can be attached to just about anything and can be used for a list of applications from inventory control to access management.

In performing this analysis we ask two basic questions: (1) Should wireless communications equipment be allowed into nuclear power plants? (2) If so, what criteria should be used for selecting the proper wireless equipment for each of the various areas and applications of the plant? We pose the second question because we are almost certain that the answer to the first question is “yes.” To answer these questions about wireless technology it is necessary to have specific knowledge about the available products, their utility, and their potential for harm relative to the operation of a nuclear power plant.

RF sensor technology is becoming more popular as wireless technologies mature. Though sensors are basically an application, they are mentioned separately because a separate Institute of Electrical and Electronics Engineers, Inc., (IEEE) family of standards cover their design, one of which is a wireless sensor standard. RF sensors vary greatly in size and complexity, and therefore they can range from custom, low-power RF components, to simple nodes on an 802.11 network, to high-power long-range custom RF components.

2. TECHNOLOGY BACKGROUND

Deployment of wireless technologies within a nuclear power plant should be based on needs. The designers and decision makers can then step through a decision process to determine the proper technology to deploy and the best system design utilizing that technology. For example, perhaps the first question to ask once the requirements are clear is, “Is there a commercial product suitable to meet the requirements?” Perhaps a more appropriate form of the question is, “Is there a commercial product that comes sufficiently close to meeting the requirements that it can be tailored to meet all the requirements?” For example, wireless technologies that connect to a standard Ethernet network can often be modified from the wired LAN side to increase functionality and security.

2.1 Throughput vs Range

The basic measure of performance of a data communications system is energy per bit. For a given design, it generally takes a certain level of energy to distinguish each data
bit from the noise around it. It follows, then, that system design considerations for the length of the bit (data speed), the power output, the design of the antenna, the modulation technique, the length of the link, etc., all have impact on the range vs throughput metric.

Figure 1 shows typical ranges vs throughput curves of WLAN cards. In comparing these units, it is also informative to make note of the power consumption. All of the power consumption values listed apply during transmission. A typical node of this type can deliver 1 Mbps over a range of 300 ft for a power consumption of about 1 to 2 W.

![Figure 1](image.png)

**Fig. 1** Graph of throughput vs indoor range for different output powers.

An updated WiFi chipset has recently been announced by Airgo (Temme, 2003) that promises to increase range between 2 and 6 times that of competing WLAN chipsets. It also promises a dramatic increase in data rate. Operational devices are not available at the time of this writing; therefore, this chipset is not represented in Fig. 1. Devices operating at the new nonstandard data rates will not interoperate with standard 802.11-b devices; although because of the 802.11 carrier sensing feature, they could co-exist on the same channel.

2.2 Modulation Techniques Making a Difference

Frequency hopping spread spectrum (FHSS), direct sequence spread spectrum (DSSS), and orthogonal frequency division multiplexing (OFDM) modulations represent most of the currently supported wireless networking product lines. Table 1 shows a comparison of a few of the physical layer choices adopted within IEEE 802 as well as a couple of other wireless standards. [IS-95 refers to the cell-phone code division multiple access (CDMA) standard.] The other network sizes shown include personal area networks (PANs), LANs, and wide area networks (WANs).
Table 1  Overview of wireless standards.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Modulation</th>
<th>GHz</th>
<th>Size</th>
<th>Maximum Mbps</th>
</tr>
</thead>
<tbody>
<tr>
<td>IS-95</td>
<td>DSSS</td>
<td>1 ±</td>
<td>Cell</td>
<td>1</td>
</tr>
<tr>
<td>P802.15.1</td>
<td>FHSS</td>
<td>2.45</td>
<td>PAN</td>
<td>0.7</td>
</tr>
<tr>
<td>P802.15.4</td>
<td>DSSS</td>
<td>0.868–0.915</td>
<td>PAN</td>
<td>0.25</td>
</tr>
<tr>
<td>P802.16b</td>
<td>DSSS</td>
<td>5</td>
<td>WAN</td>
<td>54</td>
</tr>
<tr>
<td>802.11a</td>
<td>OFDM</td>
<td>5</td>
<td>LAN</td>
<td>54</td>
</tr>
<tr>
<td>802.11</td>
<td>FHSS/DSSS</td>
<td>2.45</td>
<td>LAN</td>
<td>1, 2</td>
</tr>
<tr>
<td>802.11b</td>
<td>DSSS</td>
<td>2.45</td>
<td>LAN</td>
<td>5.5, 11</td>
</tr>
</tbody>
</table>

Because OFDM uses essentially all of the frequencies (with minimum spacing) all of the time, it appears to have the best spectral efficiency (bits/s/Hz) of the three methods, especially compared with typical implementations of FHSS and DSSS. This is particularly true in the case of adaptively modulated OFDM formats (like those employed in the IEEE 802.11a protocols and in several wireless versions proposed for the developing IEEE 802.16 MAN standard). Here, each OFDM carrier may be individually modulated via binary phase-shift keying (BPSK) or multilevel quadrature amplitude modulation (n-QAM) constellations (usually with $n = 4, 16, 64, \text{or} 256$), thus yielding even higher spectral efficiency figures when the link has a high signal-to-noise ratio. In general, direct-sequence has the second-best spectral efficiency, and frequency hopping is third in this list.

Table 2 shows some broad generalizations about the three technologies. Although controversial, these results are generally true (especially if adjacent-cell reuse is not considered). OFDM is more optimal for a few nodes streaming large amounts of data, while DSSS is more optimal for many users using fewer data per node. Their respective abilities to adapt to the RF channel and interferers will determine their effective range. The point of this table is to give general guidance. The trade-offs between these technologies are very application- and product-dependent.

Table 2  Comparison of RF technologies.

<table>
<thead>
<tr>
<th>Typical rank</th>
<th>Spectral efficiency (bits/s/Hz)</th>
<th>Noninterfering</th>
<th>Power required</th>
<th>Data reliability</th>
<th>Effective range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Best</td>
<td>OFDM</td>
<td>DSSS</td>
<td>FHSS</td>
<td>OFDM</td>
<td>OFDM</td>
</tr>
<tr>
<td>Median</td>
<td>DSSS</td>
<td>FHSS</td>
<td>DSSS</td>
<td>DSSS</td>
<td>DSSS</td>
</tr>
<tr>
<td>Worst</td>
<td>FHSS</td>
<td>OFDM</td>
<td>OFDM</td>
<td>FHSS</td>
<td>FHSS</td>
</tr>
</tbody>
</table>

It is expected that in the near future, devices using ultrawide band (UWB) will become part of the more widely accepted open standards. In addition to communications systems, UWB is useful for precise measurement of distances, determining precise locations, device tracking, and for obtaining the images of hidden objects. It is not difficult to imagine how some of these uses could be effective in and around a nuclear power plant. In general, UWB emits a very short pulse of RF or microwave energy much like a radar pulse. UWB systems may use time, phase, or amplitude modulation to the
carrier wave to convey information. The same Fourier windowing transformation applies to UWB that applies to any digital modulation. If the UWB pulse uses a rectangular time window, then the spectrum would have the same classic \((\sin x)/x\) shape as that of DSSS. However, because the time windows are much shorter (<1 ns rather than >10 \(\mu\)s), the spectrum is 10 to 100 times wider. Most DSSS systems have a main lobe that is 1 to 100 MHz wide. However, UWB systems can have main lobes that are several gigahertz wide.

3. TECHNOLOGY AND PRODUCT IMPLEMENTATIONS

Several types of components are used in setting up a network infrastructure for a plant. Figure 2 shows the major components of a diverse network that includes wireless and tethered components providing generic data access, sensor-specific communication, and asset visibility.

![Components of a diverse network](image)

**Fig. 2** Components of a diverse network.

4. EMC ISSUES

Good spectrum management is important for the overall successful deployment of wireless technologies. For example, though not a doomsday scenario, the potential for interference between 802.11 and Bluetooth networks is very real. In addition, it is a two-way street; each can interfere with the other. This interference is most likely to cause issues when the devices are collocated, which is exactly the case in an office where one individual is attempting to use more than one of these technologies. The severity of the interference depends on the proximity of the devices. With more than 6 ft of separation between devices, there is virtually no interference. As you move the devices closer
together, “there’s a smooth, graceful degradation” in performance, according to John Drury, WiFi marketing manager for 3Com (Drury, 2001).

It can be seen from IEEE 802.15.2 (2003) that 24 of the 79 Bluetooth channels are susceptible to interference from a single operable 802.11b network. This interference shows up as an increase in latency and would be most notable by voice applications. The converse of this is the Bluetooth signal interfering with 802.11, causing reduced data rates (and therefore increased latency). IEEE 802.15.2 (2003) defines coexistence mechanisms from both collaborative and noncollaborative perspectives. This is a new standard, and it will likely be a while before products are available for deployment.

Bluetooth interference with 802.11g networks is similar, although there are differences in modulation type between 802.11b and 802.11g. Standard 802.11g takes the channel used in 802.11b and divides it up into 52 equal subcarriers that are 312.5 KHz wide. These subcarriers are selected to be orthogonal to each other, so they can be spaced closely together. Four of the subcarriers are dedicated to provide pilot signals, which are used for phase and amplitude references when demodulating the remaining subcarriers. The 802.11g signal is most sensitive to interference at the frequencies of these pilot subcarriers, especially the ones that fall at ±2 MHz from the center frequency.

The bottom line on 802.11 and Bluetooth interference is that it is a large enough issue to require action by the standards bodies. Because the ISM band is a nonlicensed band, one can expect new technologies to emerge over time that require a new look at interference.

5. SECURITY

Security is a major issue for nuclear power plants—second only to safety. The issue of wireless communication security is fraught with real problems as well as perceived problems. The real problem is that wireless communication (as opposed to wired communication) is not confined to a conductive path that can be easily seen or easily controlled. Therefore, the signals can be intercepted at locations that may not be obvious.

There must be a layered defense approach to security. No one security measure makes a network impenetrable. Combinations of the following measures should be employed where possible: password protection, encryption, administrative controls, network diversity/segmentation, firewalls, access point management and signal strength management.

It should always be assumed that any information that traverses a wireless network will be subject to eavesdropping. To compound this concern, the encryption technique specified in the early 802.11 standards is weak and susceptible to compromise. An appropriate level of additional encryption should be deployed on top of that provided by the 802.11 standard.
The term “administrative controls” refers to policies instituted to control what types of equipment, which categories of personnel are allowed to use them, and restrictions on locations where they may be used.

For added security, networks should be diversified and hierarchical. That is, regions of the network should be separated into domains that are separated by some level of firewall protection or traffic monitoring. Information of like sensitivity should be placed on network segments that are protected from other network segments containing less sensitive information. Wireless devices should be treated as if they are untrusted devices. Establishing this mindset will help prevent the placing of inappropriate information on the wireless networks. It will also help in placing the wireless network in a position in the overall network architecture where it can be properly watched and protected. It is wise to place some sort of firewall device between the wireless network segments and the wired network.

Another layer of defense is to control the strength of radio signals that reach the public-access boundary of the facility. Such controls might include the use of directional antennas, power-controlled circuits, or special radio modulation methods such as spread spectrum. To accomplish this, propagation analysis should be conducted and verified with field strength testing. In addition, routine spectrum sweeps should be conducted to verify that new unauthorized wireless networks or devices have not been deployed.

6. IMPLEMENTATION CONSIDERATIONS AND RECOMMENDATIONS

One should not deploy a wireless technology in any environment without first thinking through all the issues and having a plan to resolve the issues that are relevant to the particular environment of interest. Any RF system must be analyzed for RF compatibility with surrounding systems from an intermodulation and interference perspective. Locations of transmitters must also be given adequate thought and planning. The desired coverage area needs to be defined and a site analysis developed. If possible, a propagation analysis should be conducted; at a minimum, field tests should be conducted once the RF equipment is identified.

Aside from these common issues, each wireless technology brings with it issues that are unique to that technology. WLAN provides a convenient way to connect computing devices to each other and/or to a facilities network. The fact that it involves computing devices (laptop computers, palm computers, desktop computers, etc.) presents unique implementation issues. The proliferation of mobile computing devices throughout industry makes them accessible not only to facilities with a need to communicate remotely but also to persons with intent to do harm. This, coupled with the fact that RF signals do not obey political boundaries, makes this technology susceptible to hacking and other abuse.

The sensitivity of data being passed on the WLAN and the sensitivity of information residing on WLAN nodes (even if it is not transmitted) must be considered carefully. Nodes on a WLAN are susceptible to hacking from other nodes on the WLAN, whether or not they are authorized. Careful administration of the individual client
computers on a WLAN is critical to prevent their being exploited. This should include the deployment of personal firewall protections on each node.

RFID tagging technology could soon find its way into nuclear power plants. RFID tags themselves can be either active or passive. They absorb energy from an interrogator and respond with a specific set of information. A complete RFID system will include the tags as well as the interrogation equipment. Frequency ranges used by RFID systems include those used by 802.11b and Bluetooth technologies (2.4 GHz to 2.5 GHz), as well as lower frequencies, 30 KHz to 500 KHz and 850 to 950 MHz. Again, it is emphasized that successful use of wireless technologies requires proper coordination and planning of all systems utilizing the spectrum.

CONCLUSIONS

Wireless technologies have matured to the point of being viable candidates for use within nuclear power plants. Regardless of the use for which they are deployed—basic computing, device tracking, or remote sensing applications—such technologies should not be deployed without due consideration of interference and security concerns.

ACKNOWLEDGMENTS

Research was sponsored by Oak Ridge National Laboratory, managed by UT-Battelle, LLC, for the U.S. Department of Energy under contract DE-AC05-00OR22725.

REFERENCES

