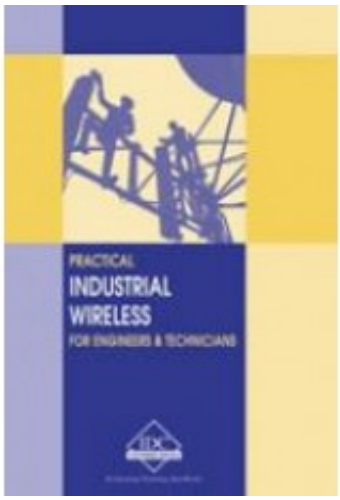
IDC Technologies - Books - 1031 Wellington Street West Perth WA 6005

Phone: +61 8 9321 1702 - Email: books@idc-online.com

WC-E - Industrial Wireless for Engineers and Technicians



Price: $65.95

Ex Tax: $59.95

Short Description

The most important objective of wireless communications networks must be to achieve similar capacities, bandwidths, responsiveness and availability to that of wire-based communications systems. This manual covers the essential areas of robust wireless links, correct integration with the wired communications systems, and proper data security. Apart from covering wireless basics, this manual also provides an in-depth coverage of the main industrial wireless technologies in use today - radio modems, IEEE 802.11 wireless LANs (Wi-Fi) and IEEE 802.15.4 wireless PAN technology as implemented by a multitude of process control system vendors. This manual should give you a clear understanding of the choices available to you in designing and implementing your own industrial wireless network.

Description

The most important objective of wireless communications networks must be to achieve similar capacities, bandwidths, responsiveness and availability to that of wire-based communications systems. This manual covers the essential areas of robust wireless links, correct integration with the wired communications systems, and proper data security. Apart from covering wireless basics, this manual also provides an in-depth coverage of the main industrial wireless technologies in use today - radio modems, IEEE 802.11 wireless LANs (Wi-Fi) and IEEE 802.15.4

wireless PAN technology as implemented by a multitude of process control system vendors. This manual should give you a clear understanding of the choices available to you in designing and implementing your own industrial wireless network.

Table of Contents
Download Chapter List

Table of Contents

First Chapter
Practical Industrial Wireless for Engineers and Technicians - Introduction

1 Introduction

This chapter serves as an introduction to topic of Industrial Wireless systems as well as the OSI model. Wireless technologies such as IEEE 802.3 (Wi-Fi) typically implement the lower two layers of the OSI model, and it is helpful if this functionality can be understood against the backdrop of the complete OSI protocol stack.

Learning objectives

After studying this chapter you will:

- Have a picture of the current overall trends in Industrial Wireless systems
- Understand the relevance of WINA and the ISA-SP100 initiatives
- Understand the concept of the OSI model and its relevance to wireless networks

1.1 Introduction

Wireless systems in the Industrial arena is nothing new. For years, wireless point-to point systems have been used in Supervisory Control and Data Acquisition (SCADA) systems in the oil, gas and electrical power generation sectors. Until recently the more ‘modern’ technologies such as IEEE 802.11 (Wi-Fi) and IEEE 802.15 (e.g. IEEE 802.15.1 Bluetooth) have been firmly entrenched in the IT and consumer markets, but not so much in the Industrial world. One of the advantages of the newer systems is that they operate in the unlicensed Industrial, Scientific and Medical (ISM) bands.

However, just as Ethernet has come of age and is rapidly penetrating the factory environment, wireless technologies are being accepted in the Industrial world. The ARC automation research group predicted in 2006 that the use of wireless technologies in the industrial world would grow by around 26% per annum. There are specific technologies that should be singled out:

- IEEE 802.11 is being used more and more as a wireless extension to Ethernet in a plant environment. The basic technology does, however, have a few inherent drawbacks when used in a plant and here (as in the case with Ethernet). In this regard vendors have taken the lead by developing enhanced Industrial versions that are backwards compatible with standard Wi-Fi products. An example is the IWLANsystem by Siemens
- IEEE 802.11 products in wireless mesh networks have been around for several years, for example in traffic control networks. Unfortunately the standard does not cater for mesh applications yet (the IEEE 802.11s amendment should be available in 2007) so all mesh systems available today (be it single, dual or multi-radio mesh) are proprietary by nature
- IEEE 802.15.4 has also become extremely popular in Industrial wireless mesh networks because of its ease of use and inherent reliability and redundancy. Several vendors are offering wireless mesh products based on IEEE 802.15.4, including Honeywell, ABB and Emerson. Revision 7 of the HART specification includes WirelessHART, a wireless mesh extension to HART

An Industrial environment, however, poses several challenges to reliable, secure wireless data transmission. These include obstacles to radio propagation (e.g. metal barriers, concrete walls), extreme temperatures, Intrinsic Safety requirements, interference and multi-path situations.

1.2 WINA and ISA-SP100

1.2.1 WINA

The Wireless Industrial Networking Alliance (WINA) was founded in 2002 and is a coalition of industrial end-user companies, technology suppliers, industry organizations, software developers, system integrators, and other parties involved in the advancement of wireless systems for Industrial applications. In this regard they aim to identify, recommend, and certify appropriate wireless technologies, to focus on customer requirements, to promote effective standards,

regulations, and practices, and to quantify and communicate the benefits and potential impacts of wireless technologies.

Their stated objectives include:

- Influencing and supporting applicable standards
- Developing user-friendly information materials
- Forming industry partnerships to sponsor wireless plant demonstrations
- Supporting Web-based education and demonstration projects
- Certifying systems in specific applications
- Demonstrating robustness and reliability
- Reducing operating costs
- Defining essential requirements and working with industry alliances and standards bodies to achieve them

Technologies scrutinized by WINA include, but are not limited to, Zigbee, IEEE 802.11, IEEE 802.15.4, Bluetooth, P1451.1/2/3/4/5, and UWB.

1.2.2 SP-100

The SP-100 Wireless Systems for Automation standards committee of ISA (the International Society for Measurement and Control) is establishing standards, recommended practices, technical reports, and related information to define procedures for implementing wireless systems in the automation and control environment. The focus is on the field level. There are currently two working groups within ISA-SP100, namely SP100.11 and SP100.14.

The SP100.11 workgroup will define wireless connectivity standards addressing a wide range of applications optimized, but not restricted to, the performance requirements of control applications. These range from closed loop PID control through open loop manual control. The SP100.14 working group, on the other hand, will define wireless connectivity standards optimized for the unique performance and cost requirements of a wide range of industrial logging, monitoring, and alarming applications.

1.3 The OSI concept

A communication framework that has had a tremendous impact on the design of LANs and WLANs is the Open Systems Interconnection (OSI) model of the International Organization for Standardization (ISO). The objective of this model is to provide a framework for the co-ordination of standards development, and allows for existing as well as evolving standards activities to be set within that

common framework.

The various technologies described in this manual relate to different layers of the OSI model, for example:

- IEEE 802.11(Wi-Fi): Physical layer (OSI layer 1) and MAC sub-layer of Data Link layer (lower half of OSI layer 2)
- IEEE 802.2: LLC sub-layer of Data Link layer (upper half of OSI layer 2)
- IEEE 802.3 (Ethernet): Same as Wi-Fi
- IP: OSI layer 3
- TCP: OSI layer 4

For that reason a quick review of the OSI model basics is a necessity. Faced with the proliferation of closed network systems, the ISO defined a ‘Reference Model for Communication between Open Systems’ (ISO 7498) in 1978. This has since become known as the ‘OSI model’. The OSI model is essentially a data communications management structure that breaks data communications down into a manageable hierarchy (‘stack’) of seven layers. Each layer has a defined purpose and interfaces with the layers above it and below it.

By laying down functions and services for each layer, some flexibility is allowed so that the system designers can develop protocols for each layer independently of each other. By conforming to the OSI standards, a system is able to communicate with any other compliant system, anywhere in the world.

The OSI model supports a client/server model and since there must be at least two nodes to communicate, each layer also appears to converse with its peer layer at the other end of the communication channel in a virtual (‘logical’) manner. The concept of isolation of the process of each layer, together with standardized interfaces and peer-to-peer virtual communication, are fundamental to the concepts developed in a layered model such as the OSI model. This concept is shown in Figure 1.1.

Figure 1.1
OSI layering concept

The actual functions within each layer are provided by entities (abstract devices such as programs, functions, or protocols) that implement the services for a particular layer on a single machine. A layer may have more than one entity; for example a protocol entity and a management entity. Entities in adjacent layers

interact through the common upper and lower boundaries by passing physical information through Service Access Points (SAPs). A SAP could be compared to a predefined ‘postbox’ where one layer would collect data from the previous layer. The relationship between layers, entities, functions and SAPs is shown in Figure 1.2.

Figure 1.2
Relationship between layers, entities, functions and SAPs

In the OSI model, the entity in the next higher layer is referred to as the N+1 entity and the entity in the next lower layer as N–1. The services available to the higher layers are the result of the services provided by all the lower layers.

The functions and capabilities expected at each layer are specified in the model. However, the model does not prescribe how this functionality should be implemented. The focus in the model is on the ‘interconnection’ and on the information that can be passed over this connection. The OSI model does not concern itself with the internal operations of the systems involved.

When the OSI model was being developed, a number of principles were used to determine exactly how many layers this communication model should encompass. These principles are:

- A layer should be created where a different level of abstraction is required
- Each layer should perform a well-defined function
- The function of each layer should be chosen with thought given to defining internationally standardized protocols
- The layer boundaries should be chosen to minimize the information flow across the boundaries
- The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy

The use of these principles led to seven layers being defined, each of which has been given a name in accordance with its purpose. Figure 1.3 shows the seven layers.

Figure 1.3

The OSI reference model

The service provided by any layer is expressed in the form of a service primitive with the data to be transferred as a parameter. A service primitive is a fundamental service request made between protocols. For example, layer W may sit on top of layer X. If W wishes to invoke a service from X, it may issue a service primitive in the form of *X.Connect.request* to X.

Figure 1.4
Service primitive

Typically, each layer in the transmitting stack, with the exception of the lowest, adds header information, or Protocol Control Information (PCI) – aka 'header' – to the data before passing it across the interface to the next layer. This interface defines which primitive operations and services the lower layer offers to the upper one. The headers are used for peer-to-peer layer communication between the stacks and some layer implementations use the headers to invoke functions and services at the adjacent (N+1 or N-1) layers.

At the transmitting stack, the user application (e.g. the client) invokes the process by passing data, primitive names and control information to the uppermost layer of the protocol stack. The stack then passes the data down through the layers of the stack, adding headers (and possibly trailers), and invoking functions in accordance with the rules of the protocol at each layer.

At each layer, the 'data' received at a certain layer (including headers from the layers above it) is referred to as a Service Data Unit or SDU. This is normally prefixed with the first letter of the name of the layer. For example, the Transport layer receives a TSDU from the Session layer. The Transport layer then processes it, adds a header, and creates a Transport Protocol Data Unit or TPDU.

At the receiving site, the opposite occurs with the headers being stripped from the data as it is passed up through the layers of the receiving stack. Generally speaking, layers in the same stack communicate with parameters passed through primitives, and peer layers communicate with the use of the headers across the network.

At this stage it should be quite clear that there is no physical connection or direct communication between the peer layers of the communicating applications.

Instead, all physical communication is across the lowest (Physical) layer of the stack. Communication takes place downwards through the protocol stack on the transmitting node and upwards through the receiving stack. Figure 1.5 shows the full architecture of the OSI model, whilst Figure 1.6 shows the effects of the addition of headers to the respective SDUs at each layer. The net effect of this extra information is to reduce the overall bandwidth of the communications channel, since some of the available bandwidth is used to pass control information.

Figure 1.5
Peer layer interactions in the OSI model

Figure 1.6
OSI message passing

1.3.1 OSI layer services

The services provided at each layer of the stack are as follows.

Application layer

The Application layer is the uppermost layer in the OSI reference model and is responsible for giving applications access to the protocol stack. Examples of Application-layer tasks include file transfer, electronic mail (e-mail) services, and network management. In order to accomplish its tasks, the Application layer passes program requests and data to the Presentation layer, which is responsible for encoding the Application layer's data in the appropriate form.

Presentation layer

The Presentation layer is responsible for presenting information in a manner suitable for the applications or users dealing with the information. Functions such as data conversion from EBCDIC to ASCII (or vice versa), the use of special graphics or character sets, data compression or expansion, and data encryption or decryption are carried out at this layer. The Presentation layer provides services for the Application layer above it, and uses the Session layer below it. In practice, the Presentation layer rarely appears in pure form, and it is the least well defined of the OSI layers. Application- or Session-layer programs often

encompass some or all of the Presentation layer functions.

Session layer

The Session layer is responsible for synchronizing and sequencing the dialog and packets in a network connection. This layer is also responsible for ensuring that the connection is maintained until the transmission is complete, and that the appropriate security measures are taken during a ‘session’. The Session layer is used by the Presentation layer above it, and uses the Transport layer below it.

Transport layer

In the OSI reference model, the Transport layer is responsible for providing data transfer at an agreed-upon level of quality, such as at specified transmission speeds and error rates. To ensure delivery, some Transport layer protocols assign sequence numbers to outgoing packets. The Transport layer at the receiving end checks the packet numbers to make sure all have been delivered and to put the packet contents into the proper sequence for the recipient.

The Transport layer provides services for the Session layer above it, and uses the Network layer below it to find a route between source and destination. The Transport layer is crucial in many ways, because it sits between the upper layers, which are strongly application-dependent, and the lower one, which are network-based.

The layers below the Transport layer are collectively known as the ‘subnet’ layers. Depending on how well (or not) they perform their functions; the Transport layer has to interfere less (or more) in order to maintain a reliable connection.

Network layer

The Network layer is the third layer from the bottom up, or the uppermost ‘subnet layer’. It is responsible for the following tasks:

- Determining addresses or translating from hardware to network addresses. These addresses may be on a local network or they may refer to networks located elsewhere on an internetwork.
- Finding a route between a source and a destination node or between two intermediate devices
- Fragmentation of large packets of data into frames small enough to be transmitted by the underlying Data Link layer (fragmentation). The corresponding Network layer at the receiving node undertakes

reassembly of the packet

Data Link layer

The Data Link layer is responsible for creating, transmitting, and receiving data packets. It provides services for the various protocols at the Network layer, and uses the Physical layer to transmit or receive material. The Data Link layer creates packets appropriate for the network architecture being used. Requests and data from the Network layer are part of the data in these packets (or frames, as they are often called at this layer). These frames are passed down to the Physical layer from where they are transmitted to the Physical layer on the destination host via the medium. Network architectures (such as Ethernet and Wi-Fi) typically encompass the Physical layer and the lower half of the Data Link layer.

The IEEE 802 networking working groups have refined the Data Link layer into two sub-layers:

- The Logical Link Control (LLC) sub-layer in the upper half, implemented as IEEE 802.2 and shared by several networking technologies such as IEEE 802.3 Ethernet, IEEE 802.5 Token Ring and IEEE 802.11Wi-Fi
- The Medium Access Control (MAC) sub-layer in the lower half, included with the Physical layer as part of the networking standards mentioned above

The LLC sub-layer provides an interface for the Network layer protocols, and controls the logical communication with its peer at the receiving side. The MAC sub-layer controls physical access to the medium.

Physical layer

The Physical layer is the lowest layer in the OSI. This layer gets data packets from the Data Link layer above it, and converts the contents of these packets into a series of electrical signals that represent ‘0’ and ‘1’ values in a digital transmission. These signals are sent across a transmission medium to the Physical layer at the receiving end. At the destination, the Physical layer converts the electrical signals into a series of bit values. These values are grouped into packets and passed up to the Data Link layer.

The required mechanical and electrical properties of the transmission medium

are defined at this level. These include:

- The type of cable and connectors used. The cable may be coaxial, twisted-pair, or fiber optic. The types of connectors depend on the type of cable
- The pin assignments for the cable and connectors. Pin assignments depend on the type of cable and also on the network architecture being used
- The format for the electrical signals. The encoding scheme used to signal ‘0’ and ‘1’ values in a digital transmission or particular values in an analog transmission depend on the network architecture being used

The medium itself is, however, not specific here. For example, Fast Ethernet dictates Cat5 cable, but the cable itself is specified in TIA/EIA-568B.

1.4 Ethernet

IEEE 802.3 Ethernet is, at present, the dominant LAN technology. It provides a set of physical media definitions, a scheme for sharing that physical media (CSMA/CD or full-duplex), and a simple frame format and hardware source/destination addressing scheme (MAC addresses) for moving packets of data between devices on a LAN. On its own, however, Ethernet lacks the more complex features required of a fully functional Industrial network. For that reason, all installed Ethernet networks support one or more communication protocols that run on top of it, and provide more sophisticated data transfer and network management functionality. It is the higher layer protocols that determine what level of functionality is supported by the network, what types of devices may be connected to the network, and how devices interoperate on the network.

For many years users have steered away from the use of Ethernet in Industrial applications, mainly because of its perceived lack of determinism. This was mainly due to CSMA/CD, which is essentially stochastic in nature. Other issues that affected its Industrial application included connectors and cabling, packaging, power supplies, switching requirements, speed, power over the cable requirements and provision for redundancy.

Modern Ethernet systems, however, differ radically from the old cable-based legacy systems. Switched Ethernet systems now operate in full duplex-mode, which, for all practical purposes, eliminates collisions. Many vendors offer industrial devices, with features such as IP67 environmental rating, rail mounting,

redundant DC power supplies, VLAN capability, prioritized switching (IEEE 802.1p/Q) and redundant ring operation.

Industry often expects device power to be delivered over the same wires as those used for communicating with the devices. The IEEE 802.3af standard allows a source device (a hub or a switch) to supply a minimum of 300 mA at 48 volts DC to field devices. Other Ethernet developments include Virtual LANs (IEEE 802.1Q), prioritized switching (IEEE 802.1p) and redundant switched rings.

Interested readers may peruse the appendix for additional information regarding Ethernet basics.

1.5 TCP/IP

The TCP/IP protocol suite consists of several protocols that provide routing services, end-to-end verification of transmitted data, and interfacing services to the stack for clients and servers.

TCP is a connection-oriented transport (OSI layer 4) protocol and runs on the two end hosts; i.e. the client host and the server host. It is a very reliable protocol, using triple handshakes to establish connections, acknowledgements and timeouts plus retransmissions to ensure correct delivery of data, and sliding windows to prevent data buffer overruns on the receiving side. This comes at a cost, in terms of protocol overheads such as header size.

UDP is a much simpler transport protocol. It is connectionless and provides a very simple capability to send ‘datagrams’ between two devices. It does not guarantee that the data will get from one device to another, does not perform retries, and does not even know if the target device has received the data successfully.

Many wireless technologies such as IEEE 802.11 only implement the lower two layers of the OSI stack, and will therefore require additional protocols such as TCP/IP. The wired Ethernet LAN to which the wireless LAN is attached will also, in most cases, use TCP/IP to implement OSI layers 3 and 4.

Once again, interested readers may turn to the appendix for more information on TCP/IP.