Introduction to the LONWORKS® System

Version 1.0

ECHELON® Corporation

078-0183-01A

Neuron Chips, LonPoint Modules, and other OEM Products were not designed for use in equipment or systems which involve danger to human health or safety or a risk of property damage and Echelon assumes no responsibility or liability for use of the Neuron Chips or LonPoint Modules in such applications.

Parts manufactured by vendors other than Echelon and referenced in this document have been described for illustrative purposes only, and may not have been tested by Echelon. It is the responsibility of the customer to determine the suitability of these parts for each application.

ECHELON MAKES AND YOU RECEIVE NO WARRANTIES OR CONDITIONS, EXPRESS, IMPLIED, STATUTORY OR IN ANY COMMUNICATION WITH YOU, AND ECHELON SPECIFICALLY DISCLAIMS ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Printed in the United States of America.
Copyright © 1999 by Echelon Corporation.

Model Number 19000

Echelon Corporation
4015 Miranda Avenue
Palo Alto, CA 94304, USA

Contents

1

Introduction

This chapter provides an overview of the LONWORKS® system.

Overview

With thousands of application developers and millions of devices installed worldwide, the LONWORKS system is the leading open solution for building and home automation, industrial, transportation, and public utility control networks. A control network is any group of devices working in a peer-to-peer fashion to monitor sensors, control actuators, communicate reliably, manage network operation, and provide complete access to network data. A LONWORKS network uses the *LONWORKS protocol*, also known as the ANSI/EIA 709.1 Control Networking Standard, to accomplish these tasks.

The LONWORKS system is based on the following concepts:

- Control systems have many common requirements regardless of application.
- A networked control system is significantly more powerful, flexible, and scaleable than a non-networked control system.
- Businesses can save and make more money with control networks over the long term than they can with non-networked control systems.

In some ways, a LONWORKS network resembles a computer data network referred to as a Local Area Network or LAN. Data networks consist of computers attached to various communications media, connected by routers, which communicate with one another using a common protocol such as TCP/IP. Data networks are optimized for moving large amounts of data, and the design of data network protocols assumes that occasional delays in data delivery and response are acceptable. Control networks contain similar pieces optimized for the cost, performance, size, and response requirements of control. Control networks allow networked systems to extend into a class of applications that data networking technology cannot reach. Manufacturers of control systems and devices are able to shorten their development and engineering time by designing LONWORKS components into their products. The result is cost effective development and consistency that allows devices from multiple manufacturers to be able to communicate.

LONWORKS networks range in sophistication from small networks embedded in machines to large networks with thousands of devices controlling fusion lasers, paper manufacturing machines, and building automation systems. LONWORKS networks are used in buildings, trains, airplanes, factories, and hundreds of other processes. Manufacturers are using open, off-the-shelf chips, operating systems, and parts to build products that feature improved reliability, flexibility, system cost, and performance.

Traditional control networks use closed islands of control linked with proprietary gateways. These gateways are difficult to install and maintain, and lock the customer into a closed, non-interoperable architecture. Ultimately, the high cost of this design approach has limited the market for control systems. The LONWORKS system is accelerating the trend away from these proprietary control schemes and centralized systems by providing interoperability, robust technology, faster development, and scale economies. Distributing the processing throughout the network and providing open access to every device lowers the overall installation and life cycle costs, increases reliability by minimizing single points of failure, and providing the flexibility to adapt the system to a wide variety of applications. For example, in the building control industry, LONWORKS networks are used to provide a common infrastructure for all building systems. This allows the building automation system designer to eliminate excessive vertical integration, which is the often the reason for vertical isolation.

Echelon manufactures over 80 LONWORKS products to help developers, system integrators, and end-users implement LONWORKS networks. These products provide a complete LONWORKS solution including development tools, network management software, power line and twisted pair transceivers and control modules, network interfaces, technical support and training.

This document is an introduction to the basics of the LONWORKS system. It begins with an overview of networks and protocols, highlights the technical aspects of the LONWORKS protocol, provides an overview of the components of the LONWORKS system, and ends with a discussion on achieving product interoperability. The next section provides a list of more detailed related reading. Many of the technical details discussed in this document are handled automatically by the protocol, the network operating system or network tools. The automatic handling of the lower level details of device communication is, in fact, one of the great strengths of the LONWORKS system.

Getting More Information

For more information on the LonWorks system, consult the following documents or browse Echelon's Web site at www.echelon.com. The documents listed below are available at www.echelon.com.

- *LonTalk® Protocol* (005-0017-01)
- *LONMARK Application Layer Interoperability Guidelines* (078-0120-01)
- *LONMARK® Layer 1-6 Interoperability Guidelines* (078-0014-01)
- *LONWORKS Network Services (LNS™) Architecture Strategic Overview* (39310)
- *LonMaker for Windows User's Guide* (39510)
- *LonManager® Protocol Analyzer User's Guide* (39600)
- *LonPoint® Application and Plug-in Guide* (078-0166-01)
- *LonPoint Module Hardware & Installation Guide* (078-0167-01)
- *PCC-10 PC Card User's Guide* (078-0155-01)
- *PCLTA-10 PC LonTalk Adapter User's Guide* (078-0159-01)
- *PCLTA-20 PC LonTalk Adapter User's Guide* (078-0179-01)
- *SLTA-10 Serial LonTalk Adapter User's Guide* (078-0160-01)
- LONWORKS System Data Sheets

2

Control Networks

This chapter explains how control networks enable the deployment of open control systems. The traditional approach to designing closed control systems is described and contrasted with the new approach of using open control networks. Finally, a hybrid approach where control network technology is used to continue the closed control system legacy is described.

The Traditional Approach

At one time, control logic was derived either through electromechanical relay panels or via pneumatic receiver/controllers. The advent of solid-state technology offered a means of reducing costs and increasing flexibility by using logic circuits to replace the wire or tubing and relays. Increasingly powerful algorithms were developed allowing tighter control over processes. However, the issues associated with adds, moves, and changes remained and grew increasingly troublesome as systems grew in size.

It was often the proprietary nature of the hardware and software that caused problems. Each manufacturer built their own systems and provided all the intelligent devices within the system. Though this provided a single point of responsibility for the system, it also 'locked-in' the customer and forced the customer to continue to deal with the original equipment manufacturer for the life of their system, whether it was a building, factory, or processing plant. Worse, the need to design, engineer, and produce an entire system limited the manufacturers to a handful of large companies. These companies tended to move slowly and quickly developed business models built upon the idea of customer lock-in. Compare the price/performance improvement of computing vs. building and industrial controls equipment and the dramatic difference becomes clear.

It has been historically difficult to interconnect digital controllers from different manufacturers. The incompatible communication protocols in the different systems focus on linking separate systems with relays, custom gateways, and programmed RS-232 ports. These interfaces, however, do not provide a detailed, seamless view into the different systems. They allowed only limited status and control information to be passed between the different systems. Fault status information could not be shared, information from different sensors was not always accessible, and systems could not adapt their responses in real-time based on the overall system status. It is possible to create intelligent building and industrial applications using gateways and custom programs, but they are typically not cost effective and reliability of the systems suffer. Once complete, the owner is forever married to those who provide the gateways and custom programming.

Figure 1 shows the centralized architecture that up until recently has been typical of most control systems in commercial and industrial applications. Sensors and actuators are wired to a sub-panel, which in turn connects to the controller panel via a proprietary master/slave communication bus. The controller panel contains a high-performance microprocessor running a custom application program that implements the control logic for all the I/O points connected to it. For large systems, this controller may communicate over another proprietary communication bus with other controllers. Sensors and actuators are typically 'dumb' I/O devices, meaning they have no internal intelligence or communication capabilities. The system typically has a proprietary human-machine interface (HMI). Every system must have a custom application program. This application is developed using a proprietary programming language and non-standard software tools that are manufacturer specific. Unfortunately, the manufacturers make no attempt to standardize the tool sets or programming models.

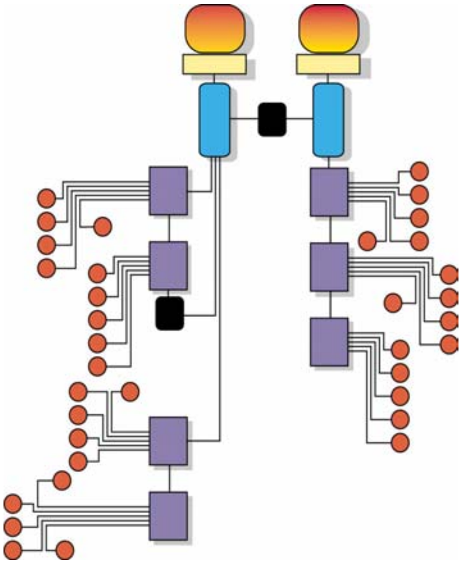


Figure 1 Centralized Architecture

Standardization requires an open control network. Much as the Internet spurned standardization for data networks, the LONWORKS system is the catalyst for standardization of control networks.

The New Control Network Approach

To understand good control network design, one must first understand the function of an open network. Put simply, an open network allows a number of intelligent devices to communicate directly with each other. No intervening supervisory controller is required to poll devices for information and then retransmit that information to other devices. No supervisory device is charged with responsibility for system-wide control algorithms.

This means that every device is capable of publishing information directly to other devices on the network. This information is transmitted by a sender in packets of data that are received by one or more receivers. An open control network is illustrated in **Figure 2**. The change from the master/slave architecture of **Figure 1** to the open architecture of **Figure 2** is exactly the type of change from proprietary hosts to open communication that has fueled the growth of the Internet.

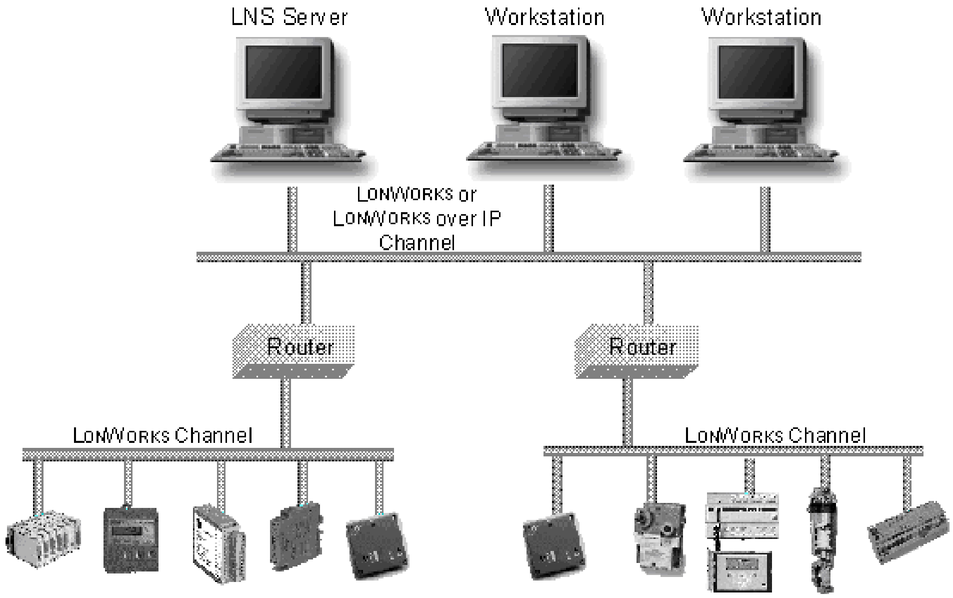


Figure 2 Open Control Network

The Transition from Data to Control Networks

Networks have been around for a number of years, yet they were not typically used for controlling devices other than large computing systems. The communication protocols employed were designed and optimized for passing large amounts of data between computers designed for batch processing. Through time, these protocols evolved to increase in scale and incorporate greater functionality and flexibility. Most, however, continued to be designed for data communication between computers or individuals.

Eventually, the cost of microprocessors reached the point that they could be incorporated into inexpensive controllers and control devices. It was at this point that design engineers began to realize the communication protocols they were using were not really tuned for optimal performance in control systems. Control networks have a number of unique requirements that make them different from data networks. These include the following:

- Frequent, reliable, secure communications between devices
- Short message formats for the information being passed
- Peer-to-peer functionality for every device
- Price points that enable small, low-cost devices

It was the need to address these control specific network requirements, together with the belief that a market standard for communications would allow interoperability that would empower the market to increase in size and efficiency, that brought about the introduction of the LONWORKS protocol.

Control Network Components

Figure 3 illustrates the key components of a control network. A control network consists of intelligent *devices* that communicate with each other using a common *protocol* over one or more *communications channels*. Network devices are sometimes called *nodes*.

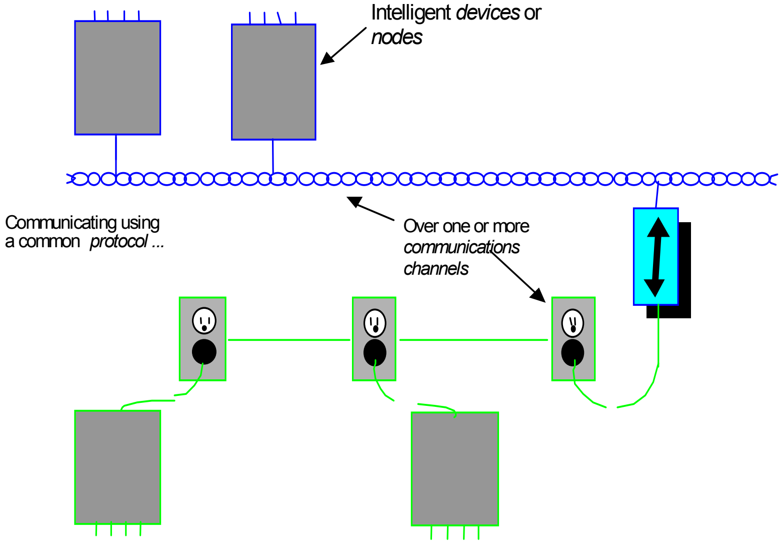

Intelligent *devices* or *nodes*
Communicating using a common *protocol* ...
Over one or more *communications channels*

Figure 3 A Control Network

Each *device* includes one or more processors that provide its intelligence and implement the protocol. Each device also includes a component called a *transceiver* to provide its electrical interface to the communications channel.

A device publishes information as appropriate to the application that it is running. The applications are not synchronized, and it is possible that multiple devices may all try to talk at the same time. Meaningful transfer of information between devices on a network, therefore, requires organization in the form of a set of rules and procedures. These rules and procedures are called the *communication protocol*, often abbreviated as the *protocol*. The protocol defines the format of the message being transmitted between devices and defines the actions expected when one device sends a message to another. The protocol normally takes the form of embedded software or firmware code in each device on the network.

The path between devices exhibits various physical characteristics and is called the *communications channel*, or simply *channel*. Different transceivers may be able to interoperate on the same channel, so channels are categorized by *channel type*, and every type of transceiver must identify the channel type or types that it supports. The choice of channel type affects transmission speed and distance as well as the network topology.

All devices connected to a specific channel must have compatible transceivers with compatible configuration. It is possible to build a transceiver for any medium, though some are more difficult to implement and therefore more expensive. Transceivers are available for a variety of communications media including single twisted-pair cable, power line, radio frequency (RF), infrared, fiber optics, and coax cable.

Using New Technologies in Old Designs

Not all control system manufacturers are ready to deliver truly open platforms. One of the more common system architectures deployed today by building, discrete, and process control manufacturers is the *hierarchical system* shown in **Figure 4**. Here we see controllers, which may even incorporate a few components of the LONWORKS system, connected to isolated networks. These networks are sometimes called *device busses* or *device networks*. The emphasis is still on providing proprietary access to sensors and actuators rather than distributing the intelligence to the field devices and providing access to any point on the network from the controllers and workstations anywhere in the hierarchy. A single vendor provides software for the proprietary controller/gateways and none of the interfaces are standardized so that tools from multiple manufactures can be used. The technology of the gateways may appear to be modern, sometimes incorporating the latest technology such as Java. The gateways sometimes communicate on an open network, also called a *control bus*. But the end-result of a hierarchical architecture is still a closed-proprietary system.

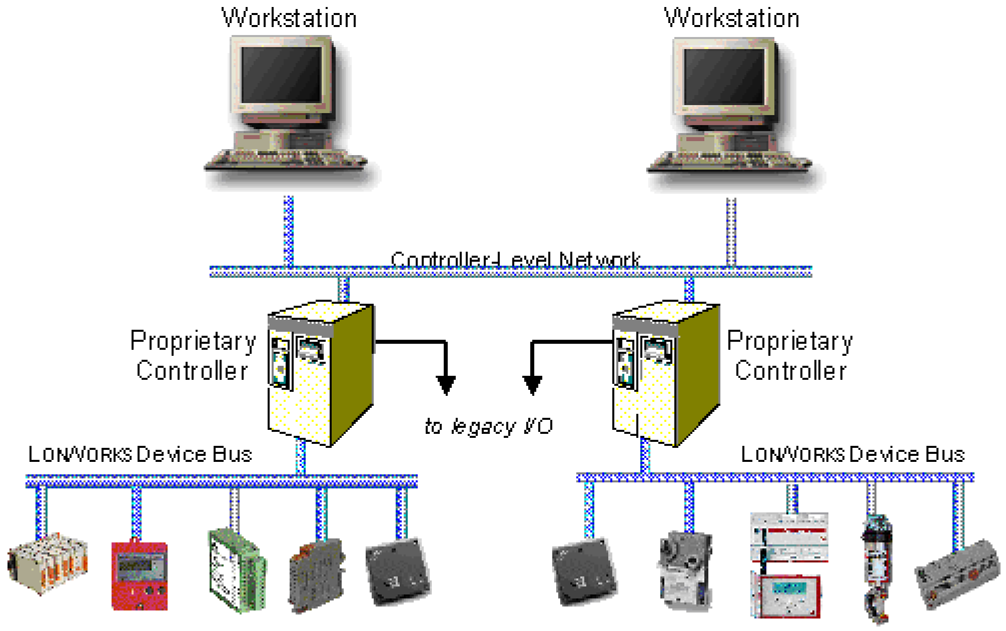


Figure 4 Typical Hierarchical System Architecture

Even when implemented with LONWORKS devices, this architecture does not capitalize on all of the power of the LONWORKS system. LONWORKS devices in this architecture typically have limited decision-making responsibility and very limited interaction with devices on other parts of the hierarchy. Their only path of communication is through the proprietary gateways. This is a step forward from a completely proprietary system, but far from true openness. The system is still closed at the next level of the hierarchy, the supervisory controllers. These devices implement most of the control relationships between I/O devices, terminal units, and other supervisory controllers. These large control panels or “black boxes” also act as a gateway for the information from the standard LONWORKS protocol into some other transport mechanism. The system controllers are often used to provide custom drivers for connectivity to another proprietary bus or to incorporate legacy equipment into the system. This is a non-interoperable, proprietary approach to solving the problem, and far from true openness. Each manufacturer has proprietary network tools for configuration and management. Further, each typically has proprietary HMI tools making it necessary for the integrator to spend time learning how to use a variety of interfaces without standards

A hierarchical system architecture is not the optimal control solution for a number of reasons. The most important reasons to the end user directly involve life cycle costs:

- *It is unnecessarily complex.* If the control system architecture were implemented with a true peer-to-peer structure, the controller-level network could be eliminated with no loss in functionality. The end-user derives no benefit from the extra level of the hierarchy and, in fact, is negatively affected by the extra cost and complexity associated with having to install, configure, and maintain a second control level network based on a different technology.
- *It is still proprietary.* Although the devices on the device network are LONWORKS and may even be built to the LONMARK® standard, the centralized controllers and the control algorithms they contain are not. They require custom programming with proprietary tools, and proprietary network management tools are required. This prohibits the end user from achieving one of the real goals of open standards: freedom of choice for modifications, additions, implementation of new functions, and maintenance.
- *It is not possible to communicate with any point, at any time, from anywhere on the network.* Because the architecture consists of multiple layers of control, it is not possible to communicate directly between devices on separate channels. Acquiring data translated through separate protocols twice and stored in a global database that may be minutes old is unacceptable. This architecture limits the information flow between devices, the ease of implementation of control algorithms, and ultimately the usefulness of the system. It can also significantly increase installation time.

The hierarchical system architecture is cumbersome and costly for end-users and systems integrators and it confuses the uninformed buyer who is led to believe they are purchasing an open system because it is based upon a technology that was conceived to provide openness. When implemented with LONWORKS networks at the lowest tier, the multi-tier control architecture is actually a collection of isolated LONWORKS networks. These LONWORKS networks contain relatively few peer-to-peer devices. In this architecture, even though there is interoperability on the device-level network, proprietary controllers provide system wide communication. LONWORKS devices are limited to sharing data directly with other LONWORKS devices on their local network only.

Instead of open network management software coordinating information transfer, there is proprietary black box software managing the controller-level network. This proprietary software is required because it attempts to hide the complexity of the multi-tier architecture from the end-user. The manufacturer can therefore charge a premium for it and he can be sure the user will require his or her services at some point in the future.

3

The LONWORKS Protocol

This chapter introduces the LONWORKS protocol and describes a few of its most important features.

Introduction to the LONWORKS Protocol

The LONWORKS protocol, also known as the *LonTalk protocol* and the *ANSI/EIA 709.1 Control Networking Standard*, is the heart of the LONWORKS system. The protocol provides a set of communication services that allow the application program in a device to send and receive messages from other devices over the network without needing to know the topology of the network or the names, addresses, or functions of other devices. The LONWORKS protocol can optionally provide end-to-end acknowledgement of messages, authentication of messages, and priority delivery to provide bounded transaction times. Support for network management services allow for remote network management tools to interact with devices over the network, including reconfiguration of network addresses and parameters, downloading of application programs, reporting of network problems, and start/stop/reset of device application programs.

The *LONWORKS protocol* is a layered, packet-based, peer-to-peer communications protocol. Like the related Ethernet and Internet protocols, it is a published standard and adheres to the layered architectural guidelines of the International Standards Organization (ISO) Open Systems Interconnect (ISO OSI) reference model. The LONWORKS protocol, however, is designed for the specific requirements of control systems, rather than data processing systems. To ensure that these requirements are met with a reliable and robust communications standard, the LONWORKS protocol is layered as recommended by the International Standards Organization. By tailoring the protocol for control at each of the OSI layers, the LONWORKS protocol provides a control-specific solution that provides the reliability, performance, and robust communications required for control applications.

The seven layers of the ISO/OSI model, along with the corresponding services provided by the LONWORKS protocol, are shown in **Table 1**. This model is often used to compare the features and functionality of communication protocols. It is not a requirement that any given protocol implement every layer of this model or even that the layers be segmented as shown in the model. A truly complete and fully scalable protocol – such as the LONWORKS protocol – provides all the services described in this model.

Table 1 ISO/OSI Reference Model

	OSI Layer	*Purpose*	*Services Provided*

7	Application	Application Compatibility	Standard Objects and Types;
			Configuration Properties;
			File Transfer; Network Services

6	Presentation	Data Interpretation	Network Variables;
			Application Messages;
			Foreign Frames

5	Session	Control	Request-Response; Authentication

4	Transport	End-to-End Reliability	End-to-End Acknowledgement;
			Service Type;
			Packet Sequencing;
			Duplicate Detection

3	Network	Message Delivery	Unicast & Multicast Addressing; Packet Routing

2	Link	Media Access and Framing	Framing; Data Encoding;
			CRC Error Checking;
			Media Access;
			Collision Avoidance & Detection;
			Priority

1	Physical	Electrical Interconnect	Media-Specific Interfaces and Modulation Schemes (twisted pair, power line, radio frequency, coaxial cable, infrared, fiber optic)

Following is a summary of the services provided by each layer:

1. The *physical layer* defines the transmission of raw bits over a communication channel. The physical layer ensures that a 1 bit transmitted by a source device is received as a 1 bit by all destination devices. The LonWorks protocol is media independent, so multiple physical layer protocols are supported depending on the communication medium.
2. The *link layer* defines media access methods and data encoding to ensure efficient use of a single communications channel. The raw bits of the physical layer are broken up into *data frames*. The link layer defines when a source device can transmit a data frame, and defines how destination devices receive the data frames and detect transmission errors. A priority mechanism is also defined to ensure delivery of important messages.
3. The *network layer* defines how message packets are routed from a source device to one or more destination devices. This layer defines naming and addressing of devices to ensure the correct delivery of packets. This layer also defines how messages are routed between the source and destination devices when these devices are on different communication channels.
4. The *transport layer* ensures reliable delivery of message packets. Messages can be exchanged using an acknowledged service, where the sending device waits for an acknowledgement from the receiver and resends the message if the acknowledgement is not received. The transport layer also defines how duplicate messages are detected and rejected if a message is resent due to a lost acknowledgement.
5. The *session layer* adds control to the data exchanged by the lower layers. It supports remote actions so that a client may make a request to a remote server and receive a response to this request. It also defines an authentication protocol that enables receivers of a message to determine if the sender is authorized to send the message.
6. The *presentation layer* adds structure to the data exchanged by the lower layers by defining the encoding of message data. Messages may be encoded as network variables, application messages, or foreign frames. Interoperable encoding of network variables is provided with standard network variable types (SNVTs).

7 The *application layer* adds application compatibility to the data exchanged by the lower layers. Standard objects promote interoperability by ensuring that applications use a common semantic interpretation of the data exchanged by lower layers. Common semantic interpretation ensures that different applications will exhibit common behavior for network variable updates. The application layer also defines a file transfer protocol that is used to transfer streams of data between applications.

All communications consists of one or more *packets* exchanged between devices. Each packet is a variable number of bytes in length and contains a compact representation of the data required for each of the 7 layers. The compact representation allows LONWORKS packets to be very short, minimizing implementation cost of every LONWORKS device.

Every device on a channel looks at every packet transmitted on the channel to determine if it is an addressee. If so, it processes the packet to see if it contains data for the device's application program or whether it is a network management packet. The data in an application packet is provided to the application program and, if appropriate, an acknowledgement, response, or authentication message is sent to the sending device.

The remainder of this chapter describes some of the most important aspects of the LONWORKS protocol.

Channel Types

The LONWORKS protocol is media-independent, allowing LONWORKS devices to communicate over any physical transport media. This empowers the network designer to make full use of the variety of channels available for control networks. The protocol provides for a number of modifiable configuration parameters to make tradeoffs in performance, security, and reliability for a particular application.

A channel is a specific physical communication medium (such as twisted pair or power line) to which a group of LONWORKS devices are attached by transceivers specific to that channel. Each type of channel has different characteristics in terms of maximum number of attached devices, communication bit rate, and physical distance limits. **Table 2** summarizes the characteristics of several widely used channel types.

Table 2 Widely-Used LONWORKS Channel Types

Channel Type	*Medium*	*Bit Rate*	*Compatible Transceivers*	*Maximum Devices*	*Maximum Distance*
TP/FT-10	Twisted pair, free or bus topology, opt. link power	78kbps	FTT-10, FTT-10A, LPT-10	64-128	500m (free topology) 2200m (bus topology)
TP/XF-1250	Twisted pair, bus topology	1.25Mbps	TPT/XF-1250	64	125m
PL-20	Power line	5.4kbps	PLT-20, PLT-21, PLT-22	Environment Dependent	Environment Dependent
IP-10	LonWorks over IP	Determined by IP network	Determined by IP network	Determined by IP network	Determined by IP network

Of particular importance is the free-topology twisted pair channel, TP/FT-10, which allows devices to be connected by single-twisted-pair wire segments in any configuration – no constraints on stub length, device separation, branching, etc; just a maximum length of cable per network segment.

Media Access

All network protocols use a *media access control (MAC)* algorithm to allow devices to determine when they can safely send a packet of data. MAC algorithms are designed to either eliminate or minimize collisions. A collision occurs when two or more devices attempt to send data at the same time. MAC algorithms that eliminate collisions are typically used in very small networks, since these algorithms do not scale well to large networks. Modern networks such as Ethernet use MAC algorithms that do not prevent, but instead minimize, collisions. The Ethernet MAC algorithm is not well suited to local control applications since it performs poorly under conditions of network overload. Existing MAC algorithms such as IEEE 802.2, 802.3, 802.4, and 802.5 do not meet all the LONWORKS requirements for multiple communication media, sustained performance during heavy loads, and support for large networks.

The LONWORKS protocol uses a unique media access control (MAC) algorithm, called the *predictive p-persistent CSMA protocol*, that has excellent performance characteristics even during periods of network overload. The LONWORKS MAC algorithm allows a channel to operate a full capacity with a minimum of collisions.

As with Ethernet, all LONWORKS devices randomize their access to the medium. This avoids the otherwise inevitable collision that results when two or more devices are waiting for the network to go idle so that they can send a packet. If they wait for the same duration after backoff and before retry, repeated collisions will result. Randomizing the access delay reduces collisions. In the LONWORKS protocol, devices randomize over a minimum of 16 different levels of delay called Beta 2 slots. Thus the average delay in an idle network is eight Beta 2 slots.

A unique feature of the LONWORKS protocol is that the number of available Beta 2 slots is dynamically adjusted by every device, based on an estimate of expected network loading maintained by each device. The number of available Beta 2 slots varies from 16 to 1008, depending on this estimate.

This method of estimating the backlog and dynamically adjusting the media access allows the LONWORKS protocol to minimize media access delays with a small number of Beta 2 slots during periods of light load, while minimizing collisions with many Beta 2 slots during periods of heavy load.

Addressing

The *addressing* algorithm defines how packets are routed from a source device to one or more destination devices. Packets can be addressed to a single device, to any group of devices, or to all devices. To support networks with two devices to tens of thousands of devices, the LONWORKS protocol supports several types of addresses, from simple physical addresses to addresses that designate collections of many devices. Following are the LONWORKS address types:

- *Physical Address*. Every LONWORKS device includes a unique 48-bit identifier called the *Neuron ID*. The Neuron ID is typically assigned when a device is manufactured, and does not change during the lifetime of the device.
- *Device Address*. A LONWORKS device is assigned a *device address* when it is installed into a particular network. Device addresses are used instead of physical addresses because they support more efficient routing of messages, and they simplify replacing failed devices. A network installation tool that maintains a database of the device addresses for the network assigns the device addresses. Device addresses consist of three components: a domain ID, subnet ID, and node ID. The *domain ID* identifies a collection of devices that may interoperate. Devices must be in the same domain to exchange packets. There may be up to 32,385 devices in a domain. The *subnet ID* identifies a collection of up to 127 devices that are on a single channel, or a set of channels connected by repeaters. Subnet IDs are used to support efficient routing of packets in large networks. There may be up to 255 subnets in a domain. The *node ID* identifies an individual device within a subnet.
- *Group Address*. A *group* is a logical collection of devices within a domain. Unlike a subnet, however, devices are grouped together without regard for their physical location in the domain. There may be any number of devices in a group when unacknowledged messaging is used; groups are limited to 64 devices if acknowledged messaging is used. Groups are an efficient way to optimize network bandwidth for packets addressed to multiple devices. There may be up to 256 groups in a domain.
- *Broadcast Address*. A *broadcast address* identifies all devices with a subnet, or all devices within a domain. Broadcast addresses are an efficient method to communicate with many devices, and are sometimes used instead of group addresses to conserve the limited number of available group addresses.

Every LONWORKS packet transmitted over the network contains the device address of the transmitting device (the *source address*) and the address of receiving devices (*destination address*) that can either be a physical address, a device address, a group address, or a broadcast address.

Multiple domains are used if the number of devices exceeds the allowed domain limit or if there exists a desire to separate the devices so that they do not interoperate. It is possible for two or more independent LONWORKS systems to coexist on the same physical channel, as long as each system has a unique domain ID. Devices in each system respond only to those packets corresponding to their domain ID and do not know about or care about packets addressed with other domain IDs. Devices also respond to packets addressed with their own physical address, which is usually known only to the corresponding network installation tools. When a physical network is shared, overall network response times will be affected due to the increased number of packets, so coordinated overall network design is required.

Message Services

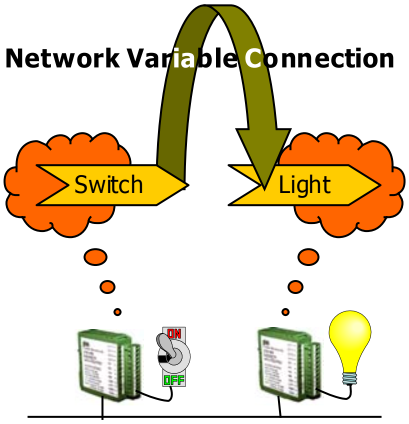
The LONWORKS protocol offers three basic types of message delivery service and also supports authenticated messages. An optimized network will often use all of these services. These services allow trade-offs between reliability, efficiency, and security, and are listed below:

- *Acknowledged Messaging*. Provides for end-to-end acknowledgement. When using acknowledged messaging, a message is sent to a device or group of up to 64 devices and individual acknowledgements are expected from each receiver. If acknowledgements are not received, the sender times out and retries the transaction. The number of retries and the timeout are both configurable.
- *Repeated Messaging*. Causes a message to be sent to a device or group of any number of devices multiple times. This service is typically used instead of acknowledged messaging because it does not incur the overhead and delay of waiting for acknowledgements. This is especially important when broadcasting information to a large group of devices, as an acknowledged message would cause all the receiving devices to try to transmit a response at the same time.
- *Unacknowledged Messaging*. Causes each message to be sent once to a device or group of any number of devices and no response is expected. This messaging service has the lowest overhead and is the most typically used service.
- *Authenticated Service*. Allows the receivers of a message to determine if the sender is authorized to send that message. Thus, authentication prevents unauthorized access to devices and is implemented by distributing 48-bit keys to the devices at installation time.

Network Variables

The LONWORKS protocol implements the innovative concept of *network variables***.** Network variables greatly simplify the tasks of designing LONWORKS application programs for interoperability with multiple vendors' products and facilitating the design of information-based, rather than command-based, control systems. A network variable is any data item (temperature, a switch value, or an actuator position setting) that a particular device application program expects to get from other devices on the network (an *input network variable*) or expects to make available to other devices on the network (an *output network variable*).

The application program in a device doesn't need to know anything about where input network variables come from or where output network variables go. When the application program has a changed value for an output network variable it simply passes the new value to the device firmware. Via a process that takes place during network design and installation called *binding*, the device firmware is configured to know the logical address of the other devices or group of devices in the network expecting that network variable, and it assembles and sends the appropriate packets to these devices. Similarly, when the device firmware receives an updated value for an input network variable required by its application program, it passes the data to the application program. The binding process thus creates logical *connections* between an output network variable in one device and an input network variable in another device or group of devices. Connections may be thought of as "virtual wires." If one device contains a physical switch, with a corresponding output network variable called `switch on/off`, and another device drives a light bulb with a corresponding input network variable called `lamp on/off`, creating a connection by binding these two network variables has the same functional effect as connecting a physical wire from the switch to the light bulb.



Network Variable Connection

- Virtual wire
- Created and changed with Network Tool
- Can be changed without reprogramming device
- Makes adds, moves, and changes easy

Figure 5 Network Variable Connection

Every network variable has a *type* that defines the units, scaling, and structure of the data contained within the network variable. Network variables must be the same type to be connected. This prevents common installation errors from occurring such as a pressure output being connected to a temperature input. Type translators are available to convert network variables of one type to another type. As described in the next chapter, a set of standard network variable types (SNVTs) is defined for commonly used types. Alternatively, manufacturers may define their own user-defined network variable types (UNVTs).

Network variables make possible *information-based control systems*, rather than old-style *command-based control systems***.** This means that in a LONWORKS system, each device application makes its own control decisions, based on information it collects from other devices about what is going on in the system. In a command-based system, devices issue control commands to other devices, so a command-issuing device, that is typically a centralized controller, must be custom programmed to know a lot about the system function and topology. This makes it very difficult for multiple vendors to design standard control devices that can easily be integrated. Network variables make it easy for manufacturers to design devices that systems integrators can readily incorporate into interoperable, information-based control systems.

Limits

Each domain in a system using the LONWORKS protocol **can have up to 32,385 devices**. There can be **up to 256 groups in a domain** and each group can have any number of devices assigned to it, except that when end-to-end acknowledgement is required, groups are limited to 64 devices. There can be **up to 255 subnets in a domain** and each subnet may have up to 127 devices. This information is summarized in **Figure 6**.

• Devices in a subnet	127
• Subnets in a domain	255
• Devices in a domain	32,385
• Domains in a network	2^{48}
• Maximum devices in system	32K x 2^{48}
• Members in a group	
♦ Unacknowledged or Repeated	No Limit
♦ Acknowledged or Request Response	63
• Groups in a domain	255
• Channels in a network	No Limit
• Bytes in a network variable	31
• Bytes in an application or foreign frame message	228
• Bytes in a data file	2^{32}

Figure 6 LONWORKS Protocol Limits

The LONWORKS Protocol Standard

Up until a few years ago, the LONWORKS protocol was only available embedded in the Neuron Chip. This ensured consistent application by all manufacturers. Now that a large number of compliant devices have been installed, Echelon Corporation has published the LONWORKS protocol and made it an open standard under the ANSI/EIA 709.1 Control Networking Standard. The protocol is therefore freely available to anyone. To get a copy of the protocol specification, access global.ihs.com and request a copy of ANSI/EIA 709.1.

The most cost-effective manner in which to implement the LONWORKS communications protocol continues to be by purchasing a Neuron Chip. The ANSI/EIA standard, however, allows any company willing to undertake the investment to implement the protocol in the microprocessor of their choice.

Summary

In summary, the variety of services provided by the LONWORKS protocol allow for enhanced reliability, security, and optimization of network resources. The features and benefits provided by these services include:

- Supports a broad range of communication media, including twisted-pair wiring, power lines, and communication over IP networks.
- Supports networks constructed with a mix of media types and communication speeds.
- Supports efficient delivery of small messages, optimizing network usage for control applications.
- Supports reliable communication, including defense against unauthorized system use.

- Eliminates single points of failure, further increasing system reliability.
- Offers predictable response times independent of network size.
- Supports low-cost implementation of devices, tools, and applications.
- Minimizes installation and maintenance costs, resulting in lower life-cycle costs.
- Supports tens of thousands of devices — but is equally effective in networks with only a few devices.
- Permits flexible and easily reconfigurable connectivity among devices.
- Allows peer-to-peer communication thus allowing its use in both centralized and distributed control systems.
- Provides an effective mechanism for product interoperability, such that products of one manufacturer can share information about standard physical quantities with those of another manufacturer.

4

Interoperability

This chapter explains how guidelines have been developed so that multiple manufacturers can easily create LONWORKS devices that interoperate with each other. This chapter also explains how specifiers, integrators, and installers can take advantage of LONMARK certification to reduce the installation cost for LONWORKS networks.

Overview

The LONWORKS system enables the development of truly interoperable devices and systems. However, since the LONWORKS components that comprise the LONWORKS system are communication-media-independent and do not prescribe how device application programs are to be structured, simply using LONWORKS components does not guarantee that LONWORKS devices from different manufacturers can interoperate in the same system. Indeed, LONWORKS components are widely used in proprietary systems such as vehicle control systems, conveyor systems, and telephone central office monitoring systems. Such systems are not afforded the full benefit of the complete LONWORKS system.

There is an important difference between a collection of interoperable devices and an open system. It is impossible to have an open system without interoperable devices, but quite possible to have a collection of interoperable devices in a closed system. In other words, interoperable devices are necessary, but not sufficient to achieve open systems. Proper network design is the additional requirement to implement a truly open system. Interoperable devices are the most basic component in the development of open systems. Thus, the LONMARK Association was formed to promote and support those manufacturers that produce interoperable products.

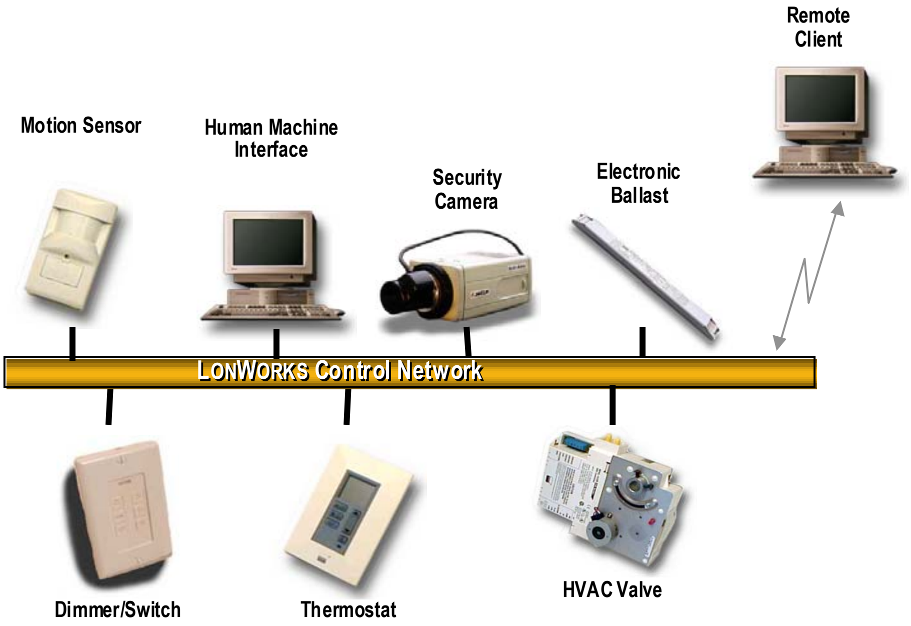


Figure 7 An Open System

The LONMARK Association

Because there are vast opportunities in many industries for interoperable products, the LONMARK Interoperability Association was formed in 1994 by Echelon and a group of LONWORKS users dedicated to building interoperable products. *Interoperability* means that multiple devices from the same or different manufacturers, can be integrated into a single control network without requiring custom nodes or custom programming. The *LONMARK Association* is dedicated to developing standards for interoperability, certifying products to those standards, and promoting the benefits of interoperable systems.

The LONMARK Association provides device level assurance of interoperability. Only LONWORKS devices that have been certified by the LONMARK Association – called *LONMARK devices* – can carry the LONMARK logo. Membership in the LONMARK Association is open to all interested companies; different dues structures exist for manufacturers, system integrators and end users. Complete information about members, current activities, and published standards may be obtained from the Association's website (www.LONMARK.org).

The LONMARK Association is governed by an Industrial Council drawn from members representing all of the interested communities. Membership in the Association is open to any company, organization, or individual committed to the development, manufacture, and use of LONMARK-certified products based on the LONWORKS protocol. The Association develops technical product specifications and guidelines, which ensure that products designed accordingly will interoperate. It also develops and publishes functional profiles which describe in detail the application layer interface, including the network variables, configuration properties, and default and power-up behaviors required for specific, commonly used control functions. Thus, the Association focuses on two areas:

1. Specification of standard transceivers and the associated physical channels.

2. Definition of standards for structuring and documenting device application programs.

Transceiver and Physical Channel Standards

The LONMARK standards for transceivers and physical channels are contained in *LONMARK Layers 1-6 Interoperability Guidelines*. Table 2.1 of that document shows all the standard physical channels for which corresponding transceivers are certified. It also provides guidelines for use of the LONWORKS protocol – buffer sizes/counts/types, address table entries, etc.

The channel types which are used most often in commercial and industrial applications are the TP/FT-10 channel type (twisted pair free topology at 78 kbps) and TP/XF-1250 channel type (twisted pair bus topology at 1.25 Mbps). The channel type used most often is residential applications is the PL-20 channel (power line at 5.4 kbps). Occasionally, the PL-20 power line type is used to leverage existing power wiring as a transmission medium in commercial and industrial applications.

Application Program Standards

The LONMARK standards for interoperable device application programs are contained in *LONMARK Application Layer Interoperability Guidelines*. These guidelines are based on *functional profiles*, which are implemented as *LONMARK objects* on individual devices. The interfaces to application programs are defined as one or more LONMARK objects. Each LONMARK object performs a well-documented function and communicates with other LONMARK objects, on the same or different devices, according to well-defined input-output interface specifications. Once a complete set of LONMARK objects has been created, the task of designing a network becomes one of selecting the appropriate LONMARK objects and connecting them.

LONMARK objects are defined as a set of one or more input and/or output network variables, with semantic definitions relating the behavior of the object to the network variable values and to a set of *configuration properties* that specify configuration data for the object. To provide for future expansion and to enable manufacturer differentiation, the LONMARK object definitions consist of mandatory network variables and configuration properties, optional network variables and configuration properties, and may consist of manufacturer-specific network variables and configuration properties. To ensure interoperability, the correct behavior of a LONMARK device cannot be dependent on its manufacturer-specific interfaces.

Standard Network Variable Types (SNVTs)

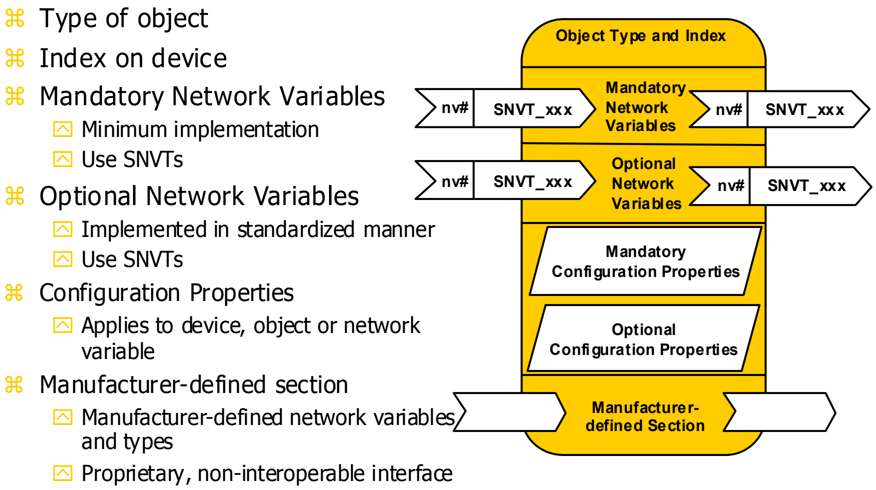
In order for applications from multiple manufacturers to easily interoperate using network variables, the data within the network variable must be interpreted in the same way. As an example, all temperature values must be transmitted over the network media in a common format, which may have been Kelvin, Celsius, or Fahrenheit, but can only be one of these for true interoperability. This is facilitated by the LONMARK Association, which has defined and published over a hundred common system variables. These are referred to as *Standard Network Variable Types* **(***SNVTs* - pronounced "snivets"). Check www.LONMARK.org for a current list and details of all SNVTs. The use of SNVTs does not mandate how data is displayed to a network tool user. For example, even though temperature values are transmitted as Kelvin or Celsius values, they may be easily displayed in Celsius or Fahrenheit under control of a network tool user.

Configuration Properties

Each LONMARK object exchanges information with other LONMARK objects only by network variables. However, most objects also require customization for a specific system application. The LONMARK guidelines specify data structures called *configuration properties* that provide standards for documentation and for the network message formats used to download the customization data to the device by network tools. The LONMARK Association defines a standard set of configuration property types; these are called *Standard Configuration Property Types* (*SCPTs*, pronounced skip-its). Manufacturers may also define their own configuration property types; these are called *User-defined Configuration Property Types* (*UCPTs*, pronounced you-keep-its). SCPTs are defined for a wide range of configuration properties used in many kinds of functional profiles, such as hysteresis bands, default values, minimum and maximum limits, gain settings, and delay times. SCPTs are to be used wherever applicable and are documented at www.LONMARK.org. In situations where there is not an appropriate SCPT available, manufacturers may define UCPTs for configuring their objects, but these must be documented in resource files according to the LONMARK standard resource file format. See *LONMARK Resource Files*, later in this chapter, for more information.

LONMARK Objects and Functional Profiles

Functional profiles may be generic, such as a simple Open Loop Sensor Object, or may be designed for specific application areas, such as HVAC or lighting systems. An example is the VAV Controller functional profile, which takes room temperature value from the network and implements a PID control algorithm to drive a damper actuator to regulate room temperature. The LONMARK Association forms task groups of interested members to design, approve, and publish functional profiles in numerous functional areas, such as HVAC, security, lighting, and semiconductor manufacturing systems. A functional profile is shown in **Figure 8**.



- Type of object
- Index on device
- Mandatory Network Variables
  - Minimum implementation
  - Use SNVTs
- Optional Network Variables
  - Implemented in standardized manner
  - Use SNVTs
- Configuration Properties
  - Applies to device, object or network variable
- Manufacturer-defined section
  - Manufacturer-defined network variables and types
  - Proprietary, non-interoperable interface

Object Type and Index
nv#
SNVT_xxx
Mandatory Network Variables
nv#
SNVT_xxx
nv#
SNVT_xxx
Optional Network Variables
nv#
SNVT_xxx
Mandatory Configuration Properties
Optional Configuration Properties
Manufacturer-defined Section

Figure 8 Functional Profile

LONMARK functional profiles describe in detail the application layer interface, including the network variables, configuration properties, and default and power-up behaviors required on LONMARK devices for specific, commonly-used control functions. Profiles standardize functions not products. Profiles therefore give industry groups universal shorthand in which to describe common units of functional behavior. This shorthand eases the specification process and enhances interoperability without compromising a specifier's ability to call for unique capabilities, or a manufacturer's ability to differentiate a product from the competition. A product can be based on one or more functional profiles.

An application program in a LONMARK device thus consists of one or several LONMARK objects each based on the definition of a functional profile, and each configured and used independently of the others. The LONMARK objects can be connected to any other objects on the network to implement desired system-level functionality. Most LONMARK devices also contain a node object, which allows its own status and the status of the other objects in the device to be monitored by network tools.

All LONMARK devices must be self-documenting, thus assuring that any LNS tool can obtain from any LONMARK device over the network all the information needed to connect the device into the system and to configure and manage that device. Each LONMARK device also must have an *external interface file* (a specially formatted text PC file with a .XIF extension), so that network tools can design and configure a network database prior to physical connection of the devices and can then commission the devices after they are installed. On its website, the LONMARK Association maintains a database of the external reference files for all LONMARK devices.

Program IDs

A *program ID* is a unique identifier for a device application that is included in every LONWORKS device. Devices that conform to the LONMARK guidelines contain a program ID in a standard format called a standard program ID. A standard program ID identifies the manufacturer of the device, the functionality of the device, the transceiver used, as well as the intended usage. Standard program IDs can therefore be used by network tools to functionally identify devices on a LONWORKS network. The fields within the standard program ID are as follows:

- *Format*. A 4-bit value defining the structure of the program ID. Program ID formats 8 and 10 - 15 are reserved for interoperable LONMARK devices, and can only be used for devices that have passed a LONMARK conformance review. Program ID format 8 is used for Standard Program IDs, and indicates a LONMARK certified device. Format 9 indicates a LONMARK compliant device that has not passed a LONMARK conformance review; it can be used for development, prototyping, and field trials prior to completing a LONMARK conformance review. The remaining fields of the program ID are interpreted identically for formats 8 and 9.
- *Manufacturer ID*. A 20-bit unique ID identifying the manufacturer of the device. This ID is assigned to a manufacturer upon request when it becomes a member of the LONMARK Interoperability Association. Manufacturers who do not yet have an ID can use manufacturer ID 0 for development, prototyping, and field trials.
- *Device Class*. A 16-bit ID identifying the device class. This ID is drawn from a registry of pre-defined class definitions. The device class indicates the primary function of the device. If an appropriate class designation is not available, one will be assigned by the LONMARK Interoperability Association upon request.

- *Device Subclass*. A 16-bit ID identifying a subclass within the device class. This ID is drawn from a registry of pre-defined subclass definitions. The device subclass indicates the transceiver type used on the device and also its intended usage, i.e. residential, industrial, commercial building etc. If an appropriate subclass designation is not available one will be assigned upon request.
- *Model Number*. An 8-bit ID identifying the specific product model. Model numbers are assigned by the product manufacturer and must be unique within the device class and subclass for the manufacturer. The model number within the program ID does not necessarily have to conform with the manufacturer's model number.

LONMARK Resource Files

LONMARK resource files are files that define the components of the external interface for one or more LONWORKS devices. These files allow network installation tools and operator interface applications to interpret data produced by a device and to correctly format data sent to a device. They also help a system integrator or system operator to understand how to use a device and to control the LONMARK objects on a device. Standard resource files are available that define the standard components used in the external interface of a device. Device manufacturers must create user-defined resource files for any user-defined components defined within the external interface of their devices.

There are four types of resource files. These are described in **Table 3**.

Table 3 LONMARK Resource Files

Type File	Defines network variable, configuration property, and enumerated types. LONMARK standard network variable and configuration property types are defined in the STANDARD.TYP file. Type files have a .TYP extension.
Functional Profile Template	Defines functional profiles that are used for describing LONMARK objects. A functional profile specifies the mandatory and optional network variable and configuration property components of a LONMARK object. Some of the optional components may not be present on a particular LONMARK object derived from the functional profile. LONMARK standard functional profiles are defined in the STANDARD.FPT file. Functional profile templates have a .FPT extension.
Format File	Defines display and input formats for network variable and configuration property types defined in a type file. Formats for the LONMARK standard network variable and configuration property types are defined in the STANDARD.FMT file. Format files have a .FMT extension.
Language File	Defines language-dependent strings. There is a separate language file for each supported language. The language the file supports determines the extension of a language file. Two language files are currently available for the LONMARK standard type files; these are STANDARD.ENU for American English

and STANDARD.ENG for British English.

Each device manufacturer that uses any non-standard types or functional profiles will typically provide resource files for their devices. The manufacturer may also supply their resource files to the LonMark Association so that they may be downloaded from www.LonMark.org.

Resource files must identify which devices they apply to. For example, the standard resource files apply to all devices. Manufacturer-specific resource files are typically associated with all devices from the manufacturer, or may be associated with a class of devices from the manufacturer, or with a specific device. This makes it possible for a user to have many resource files from many manufacturers; the files are automatically associated with the correct devices based on program ID. For more information on developing resource files, see the *LonMark Resource File Developer's Guide* available in makedrfs.zip on the LonMark website (www.lonmark.org).

5

The LONWORKS System

The LONWORKS system is much more than just a protocol and guidelines for applying the protocol. This chapter describes the components that make up the LONWORKS system, and describes how these components work together to reduce installation and system costs.

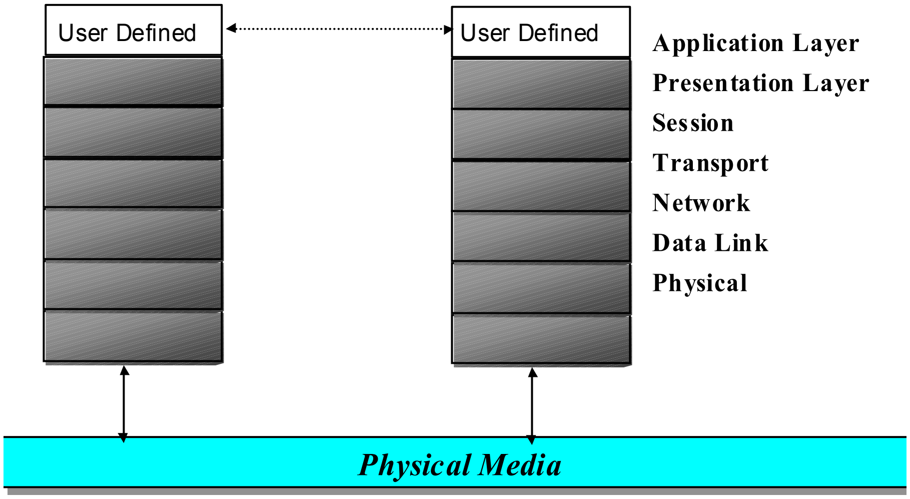
Building a System

Echelon Corporation invented the LONWORKS protocol and is the primary caretaker of the LONWORKS system. Thousands of control manufacturers currently use the LONWORKS system, though some have not made a priority of implementing open systems based upon a standard protocol and standard network management. In fact, a few large companies continue to leverage the efficiencies of the LONWORKS system while developing systems that continue to be closed and proprietary.

Echelon began the development of the LONWORKS system in 1988. The initial vision continues to drive the company forward. Create a standard, cost effective method to allow inexpensive control devices to communicate with each other effortlessly. Then use the standard communication capabilities to allow devices from multiple vendors to easily interoperate on the same network. Echelon understood that simply developing a protocol specification was not sufficient to achieve the goal of multi-vendor systems. It was necessary to build a cost-effective, standard method through which the protocol could be used and supply all the necessary development tools and networking products.

The overriding goal of the LONWORKS system is to make it easy and cost effective to build open control systems. Echelon developed the LONWORKS system believing there were three fundamental issues that had to be addressed to create interoperable products in the control market. First, a protocol optimized for control networks, but generic in its ability to work with different types of controls had to be developed. Second, the cost to incorporate and deploy this protocol in devices had to be competitive. Third, the protocol had to be introduced in such a way that implementation would not vary by vendor as this would destroy interoperability.

In order to effectively address all of these issues, Echelon Corporation set out to create a complete system for designing, creating, and installing intelligent control devices. The first step was achieved through the creation of the LONWORKS protocol, which was described in Chapter 3. Addressing the cost and deployment issues meant finding an economical way to provide implementations of the protocol to customers along with development tools. The goal of the LONWORKS system is to provide a well-integrated, optimally designed, and economical platform for creating LonWorks devices and networks. As shown in **Figure 9**, the result is a system that provides everything required by device manufacturers and system integrators with the exception of the device applications and application-specific tools. The components that make up the LONWORKS system are described in this chapter.



LonWorks provides everything but the application

Figure 9 Applications Using the LONWORKS System

The Neuron Chip

In order to achieve economical and standardized deployment, Echelon designed the *Neuron Chip*. The Neuron name was chosen to point out the similarities between proper network control implementation and the human brain. There is no central point of control in the brain. Millions of neurons are networked together, each providing information to others through numerous paths. Each neuron is typically dedicated to a particular function, but loss of any one does not necessarily affect the overall performance of the network.

To the developer and the integrator, the beauty of the Neuron Chip lies in its completeness. The built-in communication protocol and processors removes the need for any development or programming in these areas. To refer back to the ISO/OSI reference model of a communication protocol, the Neuron Chip provides the first 6 layers. Only the application layer programming and configuration needs to be provided. This standardizes implementation and makes development and configuration relatively easy.

Most LONWORKS devices take advantage of the functions of the Neuron Chip and use it as the control processor. The Neuron Chip is a semiconductor device specifically designed for providing intelligence and networking capabilities to low-cost control devices. The Neuron Chip includes three processors that provide both communication and application processing capabilities. The device manufacturer provides application code to run on the Neuron Chip and I/O devices to be connected to the Neuron Chip. Echelon Corporation designed the original Neuron Chip, and successor members of the family now designed and manufactured by Echelon's manufacturing partners. Cypress Semiconductor, Motorola, and Toshiba are all current producers of Neuron Chips. Multiple suppliers create a competitive environment for the

Neuron Chips, provide reliable sources for the chips, and help drive prices down.

The Neuron Chip is a system-on-a-chip with multiple processors, read-write and read-only memory (RAM and ROM), and communication and I/O subsystems. The read-only memory contains an operating system, the LONWORKS protocol, and an I/O function library. The chip has non-volatile memory for configuration data and for the application program, both of which are downloaded over the LONWORKS network. At the time of manufacture, each Neuron Chip is given a permanent unique-in-all-the-world 48-bit code, called the Neuron ID. A large family of Neuron Chips is available with differing speeds, memory type and capacity, and interfaces. Approximately 10 million Neuron Chips had been shipped as of late 1999, with prices less than $3 for some versions.

A complete operating system including an implementation of the LONWORKS protocol, called *Neuron Chip Firmware*, is contained in ROM on, or attached to, every Neuron Chip. Most LONWORKS devices include a Neuron Chip, which has an identical, embedded implementation of the LONWORKS protocol. This approach eliminates the "99% compatibility" problem and assures that connecting LONWORKS devices together on the same network requires little or no additional hardware. The Neuron Chip is actually three, 8-bit inline processors in one. Two execute the LONWORKS protocol; the third is for the device's application. The chip is, therefore, both a network communications processor and an application processor, significantly reducing the implementation cost for most LONWORKS devices.

Neuron Application Programs

Applications for the Neuron Chip are written in *Neuron C*. Once written, the Neuron C code is compiled into the 0s and 1s understood by the Neuron Chip and loaded into memory either on or attached to the chip. Neuron C is based on ANSI C, with the following three important extensions:

- A new statement type, the *when* statement, to introduce *events* and define task execution order.
- 37 additional data types, 35 I/O objects and 2 timer objects, to simplify and standardize device controller usage.
- Integral message-passing mechanisms for network variables and other types of messages.

The fact that it is based on ANSI C makes Neuron C easy to learn and provides a large base of existing programmers. Neuron C has a slightly different programming paradigm, however, in that it uses a programming model based on events. In other words, applications are typically triggered by events occurring elsewhere on the network or at the particular device. Therefore, the network itself is event driven. This means that LONWORKS networks have much lower traffic than other types of networks, like the typical office LAN. It also means that a device does not have to wait to be polled to report a condition.

In some complex applications, the processor speed or maximum memory of the Neuron Chip family may be insufficient to accomplish the desired function of a LONWORKS device. To accommodate these applications the

Neuron Chip has a high-speed parallel interface allowing any microprocessor to execute the application program, while using the Neuron Chip, with a special microprocessor interface application (called a *network interface* or *MIP* application), as its network communications processor. Alternatively, the open LONWORKS protocol can be ported to run directly on any processor; in such cases, a LONWORKS device does not require a Neuron Chip, but all such devices are still assigned a unique 48-bit Neuron ID.

Transceivers

Each network device contains a *transceiver*. Transceivers provide a physical communication interface between a LONWORKS device and a LONWORKS network. Transceivers simplify the development of interoperable LONWORKS devices and are available for a variety of communications media and topologies. It is important to know which transceiver is in any given product as this allows the products to interoperate directly. Products with different transceiver types can still interoperate, but this requires the use of a router. Echelon offers twisted pair and power line transceivers designed for a wide variety of applications while other manufacturers provide transceivers for radio frequency, fiber, and a variety of other media.

LONWORKS Devices

Each LONWORKS device attached to the network normally contains a Neuron Chip and a transceiver in an appropriate mechanical package. Depending on the function of the device, there may also be embedded sensors and actuators, input-output interfaces to external legacy sensors and actuators, interfaces to host processors such as PC's, or an interface to another Neuron Chip and transceiver in a router. The application program that is executed by the Neuron Chip implements the personality of the device; it may be permanently resident in ROM (read-only memory) or may be downloaded over the network into non-volatile read-write memory (NVRAM, flash PROM, or EEPROM). **Figure 10** illustrates the components of a typical LONWORKS device.

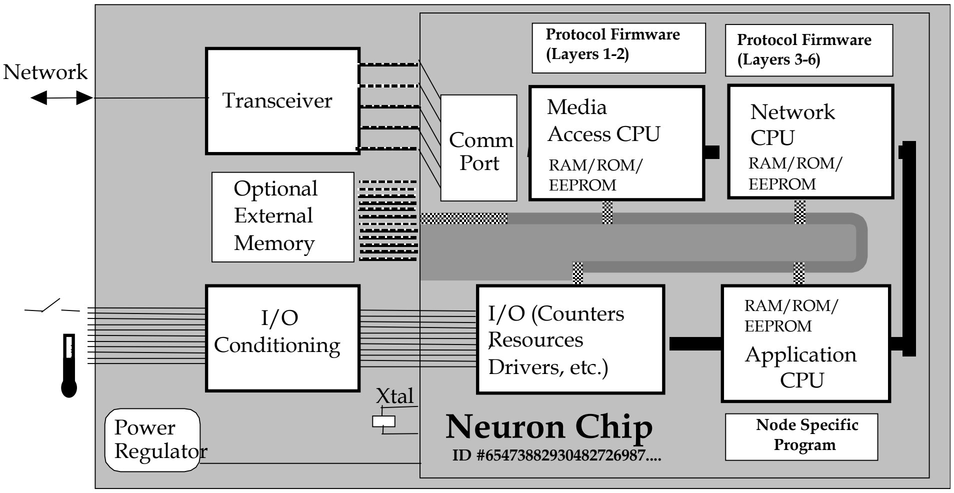


Figure 10 LONWORKS Device Components

The job of most of the devices in a LONWORKS network is to sense and control the state of the components that comprise the physical system being controlled. These are called *LONWORKS control devices* and they may have any combination of embedded sensors and actuators or input-output interfaces to external legacy sensors and actuators. The application program in the device may not only send and receive values over the network but may also perform data processing (e.g. linearization, scaling) of the sensed variables and control logic such as PID loop control, data logging, and scheduling.

Most LONWORKS devices are offered by OEM suppliers, though Echelon does offer a line of LONWORKS devices that are used to interface with non-LONWORKS sensors and actuators such as 4-20mA sensors or 0-10V actuators. These devices are called *LonPoint® Modules* and are described in the next section.

LonPoint Modules

The LonPoint System is a family of products designed to integrate new and legacy sensors and actuators, as well as LONMARK devices, into cost-effective, interoperable, control systems for building and industrial applications. The LonPoint System offers an open distributed system architecture in which every device performs some control processing and can be accessed from any location in the network.

The LonPoint interface, Scheduler, Data Logger, and Router Modules provide I/0 processing, application resources, time-of-day scheduling, sequencing, data logging, and routing for a LonPoint System. The interface modules seamlessly integrate sensors, actuators, and controller, into open distributed networks. There are five different interface modules: DI-10 Digital input Module (4 digital inputs with a status LED per input), D0-10 Digital Output Module (4 digital outputs each with a separate hand/off/auto switch and status LED), DI0-10 Digit lnput Output Module (2 digital inputs and 2 relay outputs with status LED's and a separate hand/off/auto switch for each output), AI-10 Analog Input Module (2 independent, 6-bit, analog inputs), and AO-10 Analog Output Module (2 independent 12-bit analog outputs with PID).

The SCH-10 Scheduler Module provides time-of-day control to other modules on the network. The SCH-10 module includes a flexible state machine for implementing a sequence of operations within a system or subsystem.

The SCH-10 Module may he converted into a DL-10 Data Logger by downloading the DL-10 application. The DL-10 Data Logger filters, time stamps, and logs data from other devices. The data logs can be retrieved at any time by trending or database applications for display and data analysis.

Routers

Transparent support for multiple media is a unique capability of the LONWORKS system, allowing developers to choose those media and communication methods best suited for their needs. Multiple media support is made possible by *routers*. Routers can also be used to control network traffic and partition sections of the network from traffic in another section, increasing the total throughput and capacity of the network. Network tools automatically configure routers based on network topology, making the installation of routers easy for installers and transparent to the devices.

Routers allow a single peer-to-peer network to span many types of transport media and support tens of thousands of devices. A router has two sides, each with a transceiver appropriate to the two channels to which the router is connected. Routers are completely transparent to the logical operation of the network, but they do not necessarily transmit all packets; when configured by a network installation tool, intelligent routers know enough about the system configuration to block packets that have no addressees on the far side. Using another type of router called a LONWORKS/IP router, LONWORKS systems can span great distances over wide-area networks such as the Internet.

Echelon offers *LonPoint Routers* that connect different types of twisted pair channels, as well as the *i.LON™ 1000 IP Server* for routing between twisted pair channels and an IP network such as the Internet, an intranet, or a virtual private network (VPN).

Development Tools

Development tools typically include an environment for developing and debugging applications at multiple devices, a network manager to install and configure these devices, and a protocol analyzer to examine network traffic to ensure adequate network capacity and to debug errors. Echelon's LonBuilder® and NodeBuilder™ tools can be assembled in various configurations, with a range of optional tools. Development tools make it easy and inexpensive for manufacturers to design and test individual devices for LONWORKS based control networks.

Network Interfaces, Gateways, and Web Servers

Network interfaces do not connect to control sensors and actuators, but rather have physical interfaces to external host computers such as PCs or hand-held maintenance tools. The device application program provides communication protocols to allow the host-based programs such as network tools to access the LONWORKS network. The Echelon *PCLTA-20 PC LonTalk® Adapter* is a network interface device packaged on a standard PC PCI adapter card. It plugs into the PCI bus internal to the PC, enabling access to the network for network tools such as the LonMaker tool. For laptop PCs, the Echelon *PCC-10 PC Card* provides a network interface in a compact PCMCIA PC Card format. For PCs that are isolated from the network, the Echelon *SLTA-10 Serial LonTalk Adapter* connects to a modem to provide dial-up access. Alternatively, the Echelon *i.LON 1000 IP Server* provides remote connectivity via the Internet, intranet, or virtual private network (VPN).

Gateways allow proprietary legacy control systems to be interfaced to LONWORKS systems. A gateway has a physical interface appropriate to the foreign system device or communication bus. Its application program interfaces to the proprietary communication protocol for the foreign system. The gateway translates between the two protocols as required to allow messages to pass between the two systems. It is possible in some cases for a gateway to convert the proprietary command-based messages of the foreign system to the network variable types used by the information-based LONWORKS network. A gateway, however, should not be confused as a device in the network. It is a foreign object and a link to a dissimilar system. Even if selected messages can be passed between the two systems, the link is far from seamless, provides a bottleneck, and introduces separate operating systems and network tools into the integration effort.

Web servers are a special type of gateway for providing a Web browser interface to a LONWORKS network. Web servers have a LONWORKS transceiver for attaching to a LONWORKS network, and a HTTP server that can be connected to an IP network such as the Internet. The HTTP server provides Web pages that can be viewed from any Web browser. For ease of configuration, Web servers should allow the dynamic creation of network variables on the Web server that can be connected to any network variables on the LONWORKS network, and should provide a simple way to access these network variables from the Web pages served by the Web server. The Echelon i.LON 1000 IP Server provides this type of Web server, integrated with a LONWORKS/IP router.

Network Operating Systems

A network operating system (NOS) provides a common, network-wide set of services supporting monitoring, supervisory control, installation, and configuration. The NOS also provides programming extensions for easy use of network management and maintenance tools. A LONWORKS NOS must additionally provide data access services for HMI and SCADA applications as well as remote access via LONWORKS or IP networks.

A properly designed NOS allows for synchronization services between multiple tools used by a single or multiple users. In order for a NOS to support complete interoperability, it must support LONMARK services for accessing LONMARK objects and configuration properties, as well as those for creating LONMARK dynamic network variables. Finally, the NOS must support standard plug-ins by multiple manufacturers for easy device configuration.

A properly designed NOS is not required for the normal operation of a system. The NOS provides installation and maintenance services when a network is initially commissioned or later changed, but once a network is installed, the NOS is not required to support communication between devices. This is a significant benefit of the peer-to-peer architecture of the LONWORKS system.

To provide interoperability between network tools and applications, the LONWORKS system includes a single NOS called the *LNS™ Network Operating System*. LNS provides a standard platform for supporting interoperable applications on LONWORKS networks. LNS is an infrastructure that provides the foundation for interoperable LONWORKS network tools and applications, which are products used in designing, configuring, installing, operating, and maintaining LONWORKS systems. LNS supports clients based on any platform, and servers are based on Windows NT, Windows 98, and Windows 95.

LNS uses a client/server architecture so that multiple applications can be active on a network at the same time, allowing multiple users to install devices, operate a system, diagnose problems, and make repairs simultaneously. LNS is scalable, changeable, and upgradeable.

The LNS plug-in standard encourages LONWORKS device manufacturers to provide more value to users through software components linked to their unique products. Rather than trying to develop custom programming for each project in the field, network integrators use plug-ins that configure the devices used in the project. These device plug-ins often contain built-in troubleshooting tools, user dialogues to aid or confirm configuration choice, as well as custom user interfaces to monitor or graph data held in the device. In effect, manufacturers can write smart software once to simplify the use of their products in thousands of LONWORKS networks.

Using LNS, a manufacturer's device plug-in software runs without modification in any PC, and can be seamlessly integrated with the installation tools on the PC. LNS plug-ins simplify the management of the network by masking the underlying communication mechanisms between the software component and the device. Thus, many existing devices can become fully interoperable by simply writing a plug-in. A standard interface is set for manufacturers to customize the front end, while LNS makes it possible for multi-vendor software components to work together.

Network Tools

Network tools are software applications built on top of the network operating system for network design, installation, configuration, monitoring, supervisory control, diagnostics, and maintenance. Many tools combine these functions, but the most common combinations are the following:

- *Network Integration Tools*. Provide the essential functions required to design, configure, commission, and maintain a network.
- *Network Diagnostic Tools*. Special-purpose tools to observe, analyze, and diagnose network traffic and monitor network loading.
- *HMI Development Tools*. Tools for creating human-machine interface (HMI) applications. HMI applications are used for operator interfaces to operational systems.
- *I/O Servers*. General-purpose drivers that provide access to LONWORKS networks for HMI applications not originally designed for LONWORKS networks.

Network tools based on the LNS Network Operating System are interoperable, meaning they can operate at the same time on the same network and maintain a consistent view of the devices in the network and their configuration. Echelon’s offerings for network tools are described in the following sections.

LonMaker for Windows Integration Tool

The LonMaker for Windows Integration Tool is a software package for designing, documenting, installing, and maintaining multi-vendor, open, interoperable LONWORKS networks. Based on the LNS Network Operating System, the LonMaker tool combines a powerful client-server architecture with an easy-to-use Visio user interface. The result is a tool that is sophisticated enough to design, commission, and maintain a distributed control network, yet provide the ease-of-use required by network design, installation, and maintenance staff.

The LonMaker tool provides comprehensive support for LONMARK devices as well as other LONWORKS devices. The tool takes full advantage of LONMARK features. For example, LONMARK functional profiles are exposed as graphica1 functional blocks within a LonMaker drawing, making it easy to visualize and document the logic of a control system.

The LonMaker tool conforms to the LNS plug-in standard. This standard allows LONWORKS device manufacturers to provide customized applications for their products, and have these customized applications automatically started when the LonMaker user selects the associated device. This makes it easy for system engineers and technicians to define, commission, maintain, and test the associated devices.

For engineered systems, network design is usually done off-site, without the LonMaker tool attached to the network. Network design may, however, take place on-site, with the tool connected to a commissioned network. This feature is especially desirable for smaller networks or where adds, moves, and changes are a regular occurrence.

Users are provided with a familiar, CAD-like environment for designing a control system. Visio's smart shape drawing feature provides an intuitive, simple means for creating devices. The LonMaker tool includes a number of smart shapes for LONWORKS networks, and users can create new custom shapes. Custom shapes may be as simple as a single device or functional block, or as complex as a complete subsystem with predefined devices, functional blocks, and connections between them. Using custom subsystem shapes, additional subsystems can be created by simply dragging the shape to a new page of the drawing, a time-saving feature when designing complex systems. Any subsystem can be changed to a supernode by adding network variables to the subsystem shape. Supernodes reduce engineering time by exposing a simplified interface to a set of devices.

Network installation time is minimized by the ability of the installer to commission multiple devices at the same time. Devices can be identified by service pin, bar code scanning Neuron IDs, winking, or manually entering the IDs. Auto discovery can be used for systems containing embedded networks to automatically find and commission the devices in the system. Testing and device configuration is simplified by an integrated application for browsing network variables and configuration properties. A management window is provided to test, enable/disable, or override individual functional blocks within a device or to test, wink, or set online and offline states for devices.

The LonMaker tool can both import and export AutoCAD files and generate as-built documentation. An integrated report generator and bill-of-materials generator can also be used to generate detailed reports of the network configuration.

The LonMaker tool is a single expandable tool covering the entire life cycle of the network to simplify the tasks of installers.

LonManager Protocol Analyzer

The LonManager Protocol Analyzer is a software package with high-performance network interface cards that provides tools to observe, analyze, and diagnose the behavior of installed LONWORKS networks.

The protocol analyzer can be used to collect, timestamp, and save all packets on a LONWORKS channel. Packets are saved in log files that can be later viewed and analyzed; packets may also be viewed in real-time as they are collected by the protocol analyzer.

A sophisticated transaction analysis system examines each packet as it arrives and associates related packets to aid the user in understanding and interpreting traffic patterns in their network.

Logs can be displayed in summary form with one packet per line for quick analysis, or in expanded form with one packet per window for more detailed analysis. Using data imported from an LNS database, the protocol analyzer decodes and displays packet date using the device and network variable names assigned during installation. It also provides text descriptions of each message and a description of the LONWORKS message service used to transmit it. Eliminating the need for the user to manually interpret the ones and zeros of the LonWorks protocol reduces the time and effort needed to diagnose network problems.

The user can specify capture filters to limit the packets collected. Filters can be used to limit the captured packets to packets between selected devices or network variables, or to packets using selected LONWORKS protocol services.

A traffic statistics tool provides access to detailed statistics related to network behavior. The statistics include total packet counts, error packet counts, and network loading. The statistics display provides the user with an easy-to-read summary of network activity.

LNS DDE Server

The LNS DDE Server is a software package that allows any DDE-compatible Microsoft Windows application to monitor and control LONWORKS networks – without programming. Typical applications for the LNS DDE Server include interfaces with HMI applications, data logging and trending applications, and graphical process displays.

By linking LNS and Microsoft's DDE protocol, DDE-compatible Windows applications can interact with LONWORKS devices using any of the following methods:

- Read, monitor, and modify the value of any network variable
- Supervise and change configuration properties
- Receive and send application messages
- Test, enable, disable, and override LONMARK objects
- Test, wink, and control devices

The LNS DDE Server connects LONWORKS networks to operator interfaces for control systems in buildings, factories, processing plants, semiconductor fabs, and other commercial and industrial applications. The software is compatible with Wonderware's lnTouch®, lntellution FIX®, USDATA FactoryLink®, National Instruments' LabView® and BridgeView®, Microsoft Excel, and Microsoft Visual Basic in addition to hundreds of other DDE applications. The LNS DDE Server also supports Wonderware's FastDDE protocol for improved performance with InTouch.

Once a network has been commissioned with the LonMaker for Windows Integration Tool, the LNS DDE Server automatically accesses the LNS database created by the LonMaker tool. No separate configuration step is required to use the LNS DDE Server - LNS ensures that all of the required information is already available in the LNS database.

6

Designing Open Systems

This chapter explains how network designers, consultants, specifiers, and integrators can use the components of the LONWORKS system to create open control systems.

Introduction

Designing open systems requires more than just selecting LONWORKS devices. For example, the LONWORKS system has been experiencing a strong adoption rate in the controls industry over the last few years. Despite the incorporation of the technology into a variety of products, it continues to be difficult for a consultant/specifier to design a truly open, interoperable solution. There are several reasons for this. The dominant reason, however, is the traditional approach used in designing and procuring control projects. Most building and industrial automation projects in North America continue to be implemented as multiple, isolated subsystems. Rather than viewed as a whole, building and industrial control is fragmented to match the historic procurement structure.

Fear, uncertainty, and doubt are also to blame, albeit to a lesser extent. Though every major control manufacturer continues to adopt components of the LONWORKS system at an accelerating pace, many are worried about the market changes that will be brought about by adoption of a standard network protocol. The implementation of truly open architectures will force noticeable changes in the structure of the market delivery systems. Open architectures are viewed as a possible 'Pandora's Box' to larger companies with substantial market shares. Some may find it difficult to accept the fact that open systems greatly expand markets, providing plenty of opportunity for many competitors to prosper. Others do not see the opportunity to deliver new functions and added value to both old and new customers. Despite these reservations, most manufacturers find the LONWORKS system to be a cost-effective way to build communication capabilities into their devices.

Technology advancement, however, is driving rapid changes in all types of system architectures, including control systems. In the last 20 years, centralized mainframe computers connected to dumb terminals were displaced by the distributed processing capabilities of mini-computers connected by local area networks, and those in turn were replaced by distributed peer-to peer networks of powerful personal computers. The key to the huge success of each new wave of information systems products is the widespread acceptance of industry standards for microprocessors, communication protocols, operating systems, and other hardware and software building blocks. These standards allow many manufacturers to produce high volume hardware and software products that are interoperable – they can be combined into information systems fitting any application without development of custom hardware, software, or tools. The LONWORKS system, now available as an open standard to all manufacturers, is the platform that is driving the same sweeping changes in control system architectures, displacing proprietary centralized systems with open, highly distributed, interoperable systems.

The LONWORKS system has become so prevalent in building controls that it has become common practice to use the terms 'LON' or 'LONWORKS' to describe open, multi-vendor control systems. The LONWORKS system, however, is an enabling platform, not an end-use solution that guarantees seamless interoperability. Use of components of the LONWORKS system significantly improves the ease with which an open control system can be designed and installed. Proper implementation, however, continues to require an understanding of the technology itself as well as an understanding of how to leverage the features and benefits of the technology to provide truly open systems.

The benefits to an end-user or system integrator of a LONWORKS open control system are the following:

- A wide variety of compatible, cost-effective LONWORKS devices available from multiple vendors.
- A variety of easy-to-use HMI and network tools from multiple vendors.
- Greatly reduced wiring costs.
- Short system design cycle – no custom hardware or programming.
- Greater system reliability – no single point of failure.
- Multi-vendor system maintenance options.
- Ease of implementing new functions to meet end-user needs.

This chapter is provided to assist those interested in designing open control systems using the LONWORKS system. The chapter provides information regarding the proper design of LONWORKS networks and explains how to leverage the technology to achieve open control networks.

Open System Design Requirements

The lowest cost and most powerful way to deploy LONWORKS networks is to build highly distributed peer-to-peer systems. **Figure 11** illustrates the logical concept of this approach. The physical implementation may include backbones and routers as required to mediate traffic and provide required performance, but the important point is that the workstations at the top of the figure can access any point in any device without going through a proprietary gateway. While this approach requires a paradigm shift in implementation of control architectures, it also results in lower cost, more adaptable systems. Most end users and integrators have realigned their thinking and accept this solution over hierarchical solutions. Market demand has naturally evolved to reflect the owner's desire to implement truly open systems.

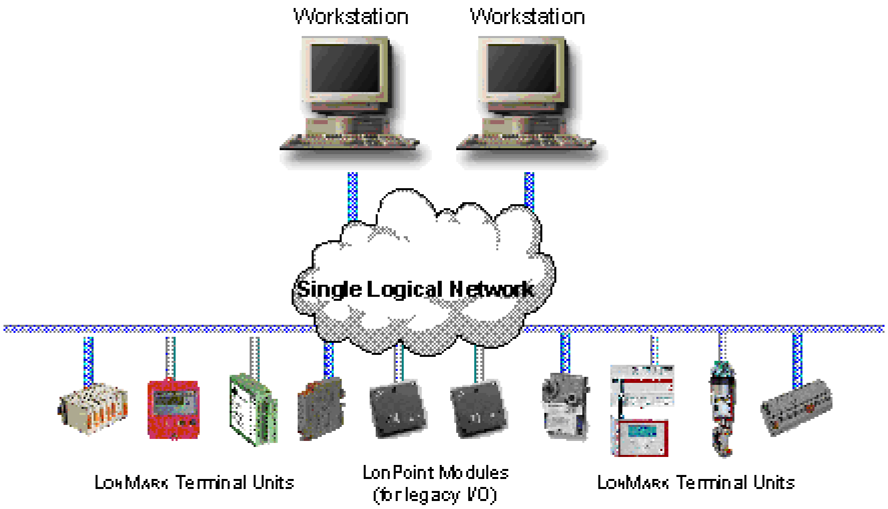


Figure 11 A fully distributed LonWorks system

The issue is no longer of whether or not to use LonWorks devices, but how to provide an infrastructure to tie the LonWorks devices and channels together and provide the functionality that has traditionally resided in a proprietary controller.

Control systems are evolving to truly open standards-based peer-to-peer architectures in a manner similar to that of the information systems markets. The LonWorks system is the crucial foundation, providing the open standards implemented in high-volume, low cost Neuron Chips. To empower the evolution of the market, however, more is needed. Consultants and specifiers must be educated concerning the use of the LonWorks system and be provided with the proper tools and information regarding products. LonMark devices such as Echelon's LonPoint devices are now available that allow consultants to distribute the control algorithms and legacy I/O interface to the LonWorks device level, eliminating the cost and complexity of proprietary supervisory controllers and controller networks.

The rapidly increasing numbers of LonMark devices available from multiple vendors deliver the ability to create a truly open, single-level, peer-to-peer control network. Some LonWorks devices now allow system integrators to integrate legacy products that do not themselves include a Neuron Chip into a truly open system. Often these modules include flexible, yet powerful, LonMark objects that can be combined to create complex control algorithms.

A New Design Paradigm

System designers must make the leap to a new paradigm and learn to spread control logic across the network. They must eliminate requirements for expensive hierarchical controllers and the cost and complexity associated with installing and maintaining proprietary supervisors which act as gateways. In a properly designed open system, there are no centralized controllers and no home-run wiring**.** LonWorks devices communicate with other devices in the system using the LonWorks protocol on whatever physical medium is best (twisted pair, AC power line, radio frequency, fiber optic cable, infrared). Each device has its own simple application program so that the control logic is distributed throughout the system; the device application is customized by setting configuration properties rather than by custom programming. In principle, every sensor or actuator in the system can be a LONWORKS device; in practice, it is often more cost effective to group small clusters of I/O points, which are physically close and part of a single control loop, into a single device.

One of the more popular arguments advanced against the open control system architecture is that a higher-speed backbone is needed to transfer data. Most of this thought process comes from trying to design control systems using the old paradigm: gather all the information in a big black box and transfer it en masse upon request. Properly designed, few control systems require throughput greater than 1 megabit per second, which the LONWORKS system readily accommodates. A good network control protocol sends short concise messages and it only sends them when they are needed. The messages are only seen within the control device community in which they are required. How often do you need to send your 10 Mbyte PowerPoint file to a sensor on your control network? The *real* reasons to consider incorporation of other transport protocols into the control system design are:

1. *Use of existing communications infrastructure*. Chances are good there is going to be a lot of fiber cable, coax cable, or twisted pairs of wires running through the building. Typically only a small percentage of the potential bandwidth is used.

2. *Increases in distance and delivery.* IP networks currently cover the planet. They are designed to provide for long distance communication. One could design standalone wide-area LONWORKS systems to deliver information from Boston to Bangladesh, but it would not be very cost effective. Why not leverage the existing networks?

3. *Leveraging existing organizational data transfer mechanisms*. Data on a control network is just that, data. People need information to gain knowledge and make decisions. Today information is gained by sitting down at a personal computer to organize and collate the data through software programs. This information is then shared with others through a network of these computers. It seems sensible to design a control system that provides the data from the device I/O level to the business level network.

With the distributed control architecture shown in **Figure 11**, users can, in fact, use high-speed backbones as a transport mechanism for their LONWORKS messages if they desire. They should simply do so using standard data transport techniques like the Internet Protocol (IP) instead of proprietary protocols. As shown in **Figure 12**, the system now uses routers between channels, instead of gateways. One such router is the Echelon i.LON 1000. These routers *tunnel* LONWORKS packets into IP packets and vice versa. If you think of a LONWORKS packet as a letter (the data) inside an envelope (the packet addressing information) and delivered to its addressees by the LONWORKS network, then a tunneling router simply encloses this LONWORKS envelope inside a bigger IP envelope, with a different kind of addressing. The wide-area network delivers this to the addressed remote router or IP device where the outside envelope is discarded and the LONWORKS envelope is placed onto the local network segment or device. This makes the system easier to install, monitor, troubleshoot, and maintain since the system is now one integrated network, with complete connectivity between all points, and no proprietary gateways to get in the way. This means, for example, that a network tool connected anywhere can interact with any device on the entire network.

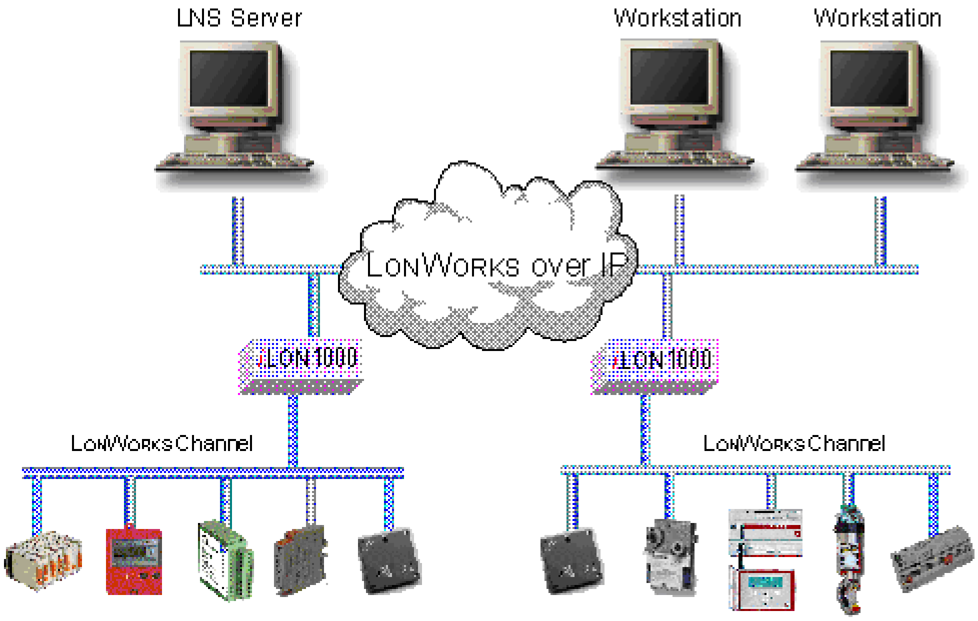


Figure 12 Open LONWORKS Network with IP Backbone

LONWORKS to IP routers provide a seamless, transparent connection from LONWORKS network segments to an Ethernet or wide-area backbone network. The end result is a consistent, powerful building automation system that is LONWORKS-based from sensors to facilities management software. Such a unified architecture can significantly reduce the life-cycle cost of the system, and can enable new functionality by taking advantage of IP technologies such as the Web and Internet.

An important benefit of this open approach is that, unlike today's architecture with gateways, custom programming of the routers is not required whenever a tool needs access to a new point on a remote segment. Another important benefit is that this approach easily extends over the Internet or an intranet, allowing geographically remote tools to access the network.

The IP backbone shown in **Figure 12** may be local to a building, factory, or plant, or may be geographically distributed using the Internet or a virtual private network (VPN). The workstations may be at the same physical locations as any of the LONWORKS channels, or may be geographically remote. This architecture is therefore useful for large systems such as multi-story buildings or large processing plants, where each floor of the building or subsystem of the plant is connected to an IP backbone. This architecture is also useful for geographically dispersed systems such as large campus sites, school districts, or enterprise-wide monitoring applications with many buildings or plants in different cities and countries.

An alternative implementation is shown in **Figure 13**. With this approach, the LNS Servers are local to each subsystem and the LNS Servers are used to provide connectivity to both the LonWorks channels as well as the IP channel. This approach does not provide the performance and flexibility of that shown in **Figure 12**, however, it may provide a cost savings for small systems that require a local PC for supervisory control or a local HMI application since the PC can support both the local application as well as provide IP connectivity. From an application standpoint, there is no difference in the application running on any of the PCs within the two networks. LNS transparently manages the differences between the two networks, and allows a system to be easily be migrated from one approach to the other.

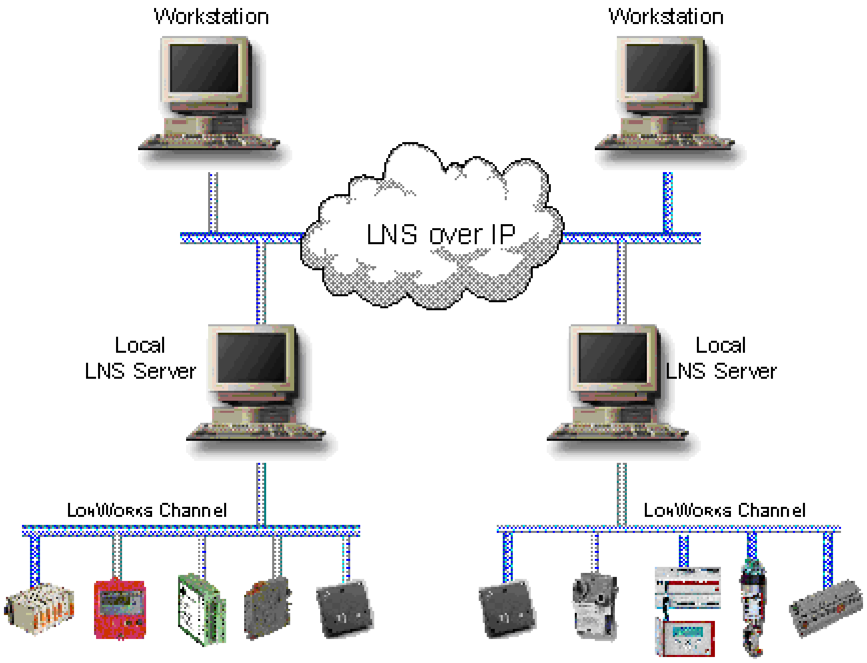


Figure 13 Open LONWORKS Network with Local LNS Servers

Hierarchical Systems

In an attempt to preserve proprietary controllers, control system manufacturers often propose a hierarchical system with different network protocols at each level of the hierarchy. For example, in industrial networks the three levels are called field busses, control busses, and device busses. In commercial building networks the two levels are frequently BACnet and LONWORKS.

The problems with the proprietary gateways required for hierarchical systems have already been described earlier in this document. However, to better highlight the problems with this hybrid approach, this section provides a more detailed discussion of hierarchical systems using BACnet and LONWORKS.

The Building Automation Control network (BACnet) standard for building control communication was developed by a project committee of volunteers. The BACnet effort was begun back in 1987 under the guidance of the American Society of Heating, Refrigeration and Air conditioning Engineers (ASHRAE). BACnet is a communications specification originally aimed at integrating islands of control. It has since evolved to encapsulate field device integration as well. BACnet includes an option to use the lower layers of the LONWORKS protocol, but BACnet imposes its own application layer on top of the LONWORKS protocol instead of the LONWORKS application layer.

BACnet is optimized for use with devices such as workstations and head-end computers that communicate relatively large amounts of data and require more sophisticated services such as alarm processing and command prioritization. The higher level of complexity and increased message size means more processing power, and therefore more costly hardware, is often required to interface BACnet devices from multiple manufacturers.

The BACnet standard is object based and there are many similarities between the BACnet and LONMARK objects. The two are not, however, interchangeable. A gateway is required to connect a system using BACnet objects with a system using LONMARK objects. BACnet objects do provide services that support the data-intensive operations normally found when connecting powerful central controllers.

One of the truly perplexing issues facing a specifier, user, or integrator in the commercial controls industry today concerns which building protocol to support. With the long awaited completion of the BACnet protocol specification, many people are tempted to rush forward in pursuit of "interoperable solutions" with BACnet. When faced with the reality of writing a specification and implementing a solution, the question becomes which standard to support: BACnet or LONMARK?

Since BACnet is optimized for use with devices that transmit large amounts of data, the hierarchical architecture is necessary when there is a need to communicate from a data-based legacy subsystem to LONMARK devices. There are cases, however, when the hierarchical system is not needed because the system is completely distributed and the LONWORKS devices communicate directly with one another.

Following the philosophy of open systems, specifiers should design and partition control systems according to the availability, functionality, flexibility, and cost-effectiveness of products.

Rather than adopt the proven LONMARK standard, some now advocate a multi-tiered approach in which systems will be based on a particular vendor's version of the BACnet protocol with some LONMARK devices thrown in for good measure. Unfortunately, there remains no independent verification of proper implementation of the BACnet protocol. It is likely existing devices are implemented in the wrong way or were never intended to interoperate with other manufacturer's devices. The effort to provide conformance for BACnet continue as recently documented in *The Development of BACnet*; "...the (BACnet) committee is now completing efforts to rewrite the 'Conformance and Specification' clause to provide the degree of constraint needed to assure interoperability. Ironically, these constraints will undoubtedly make obsolete many of the sacred cows that were originally included in BACnet for the purpose of achieving consensus."

An in depth survey of manufacturers quickly proves it is difficult, if not impossible, to find enough BACnet field-level devices to create a complete multi-vendor system. The question becomes, if LONWORKS networks are interoperable and capable of performing any control function with or without

BACnet, why use BACnet? The market should continue to embrace BACnet to the extent that it leverages the user's ability to demand openness from the proprietary legacy systems with which they are burdened. Reference the architecture in **Figure 14**.

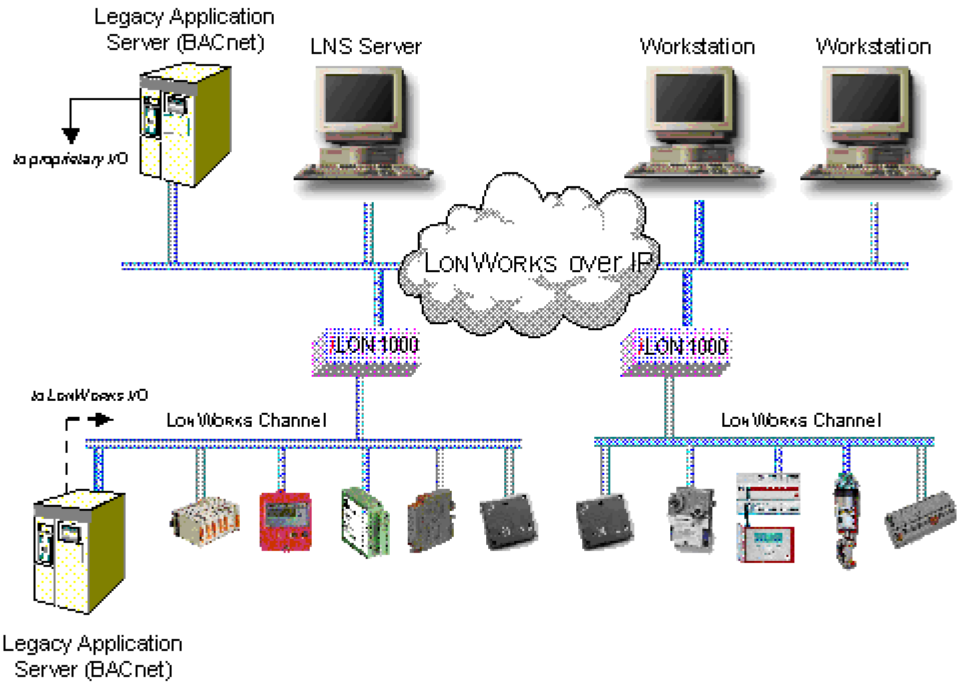


Figure 14 Open LONWORKS Network with Ethernet Backbone and BACnet Servers

In this architecture, subsystems can communicate with legacy systems using BACnet-style servers, just as they do in **Figure 14**. Unlike **Figure 14**, however, there is complete network connectivity as in **Figure 12**. In this architecture, the value of interoperability is high, since any new device can share data with any other new device no matter where they are located in the system. This approach provides the infrastructure for system installation, monitoring, troubleshooting, and maintenance and it provides the infrastructure to allow BACnet servers to communicate with one another. The BACnet servers are still gateways, however, and do not allow seamless interaction.

It is important to remember that the BACnet standard was developed by and for the U.S. HVAC industry. It does not necessarily properly address the needs of other building controls industry segments, such as lighting, security, and fire/life safety systems, nor is it likely to be widely embraced as a standard in those industries. Moreover, it certainly does not meet the needs of the industrial controls industry or many other controls industries. The LONWORKS system, on the other hand, was designed with the flexibility to meet the requirements of all industries: the LONWORKS protocol is an approved standard in many industries worldwide, and is the de facto standard in many others. As a result it can be stated with high confidence that far more manufacturers will be producing a far larger variety of control products in far higher volumes at far lower prices with far better support tools than will ever be the case for BACnet.

Design Guidelines

The LONWORKS system has without doubt played a part in increasing the expectation set for integration and openness in control systems. End users now demand the intelligent devices they buy from one vendor communicate with the devices they buy from others. They know that these devices can leverage the LONMARK guidelines to make it possible. The challenge is to educate consultants and integrators to provide for these requests.

An open control network consists of more than just open devices. Standard network management is required to install and maintain the devices. This network operating system (NOS) must contain published interfaces that are available to everyone and a large number of control manufacturers must use it. This NOS should additionally provide published interfaces for plug-ins. These plug-ins allow device software developers to cost effectively insert their application knowledge into network tools.

The following are generally accepted market realities:

- Intelligence at the point of control provides greater flexibility and reliability.
- Peer-to-peer control networks provide measurable advantages over master/slave architectures.
- Openness as defined above frees the integrator and end users to select the best in class products and services without fear of difficulty or vendor lock-in.
- TOTAL access to ALL system information from ANYWHERE in the network can best be achieved via a standard protocol used throughout the system.
- The LONWORKS system has become the platform of choice for constructing open systems in the commercial building and transportation markets, and is rapidly spreading to other markets.

The traditional control structure in many industries revolves around vertical sub-systems. Each with its own cabling, management system and service contract. Historically, the communication barrier between subsystems was addressed through extra engineering effort and complex interfaces. This makes even quasi-integration costly. These islands of automation are often tied together with string and Band-Aids to allow users to view different subsystems without having to jump from one PC to another.

Implementations like the one shown in **Figure 15** are the tradition in the commercial control market, and is typical of many industries. This implementation is not an open system under the definition given above. Open devices may actually exist on each island, but communicating with or configuring devices on other islands is far from seamless.

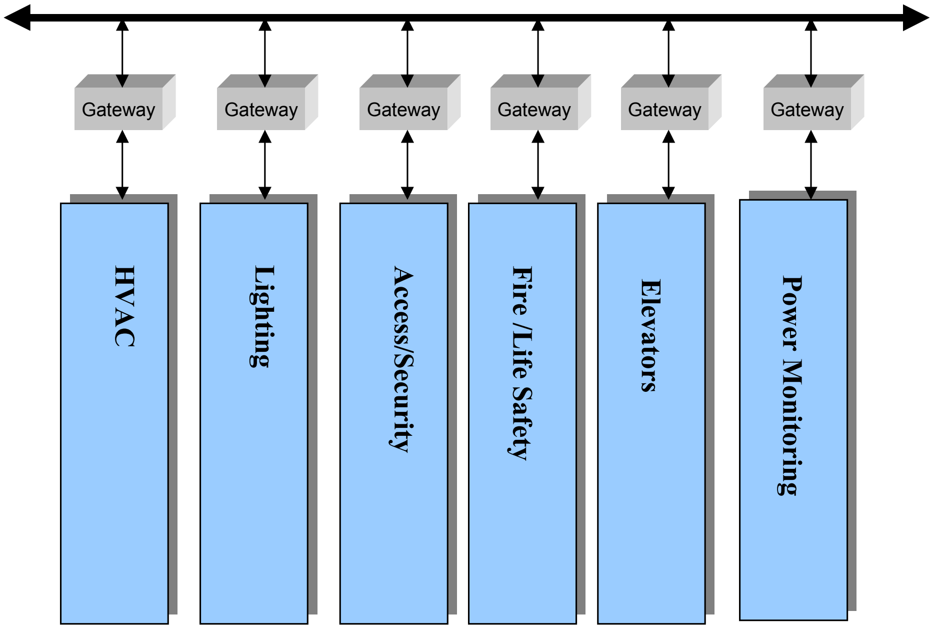


Figure 15 Islands of Automation

A Checklist for Open Control Design

Understanding the power of the open infrastructure and leveraging that power by applying it to all control functions is the key to providing holistic system control. Leveraging is achieved by eliminating the walls between control systems. Imagine eliminating the boundaries between the islands. Visualize a singular control system that leverages a common physical and logical infrastructure to provide holistic system control.

In this case, the entire system is controlled by a single control infrastructure. A standard wiring scheme allows devices to easily access and share communication media. In order for the user to use these devices easily network services are employed. Since multiple manufacturers make the devices and software on the network, the network services must adhere to a standard. Different network control systems may have different needs, however, and different users may have training in different networking tools. By creating standard network tools that adhere to the network operating system standard, different users can use the different tools on the same network. Finally, an application level standard for the exchange of information between devices exists so devices can easily communicate.

The following provides a checklist for designing system-wide open control systems.

1. Intelligent Network Wiring

The base for a system wide-open control system is intelligent wiring. Starting with this ingredient grants the integrator and end-user the ability to quickly and easily install the system as well as make additions and revisions in the future. Almost as importantly, eliminating the physical barriers between systems encourages engineers and owners to create holistic system control. Gateways and islands of automation seem even more useless when a standard wiring infrastructure exists.

To achieve this on a project means getting approval up front and planning the wiring for all system functions. This requires the owner and the consultant understand that the system can be better than the sum of it's parts if proper thought is given to holistic control in the initial stages of design.

2. Standard Network Management

Standard network management provides the necessary network services and published interfaces for the infrastructure. These services allow multiple tools from multiple vendors to coexist on the network. More importantly, it allows the various tools to share the network data.

The method to achieve a network management foundation is through the use of any control network operating system you can find that is in use by hundreds of companies around the world. A standard is of little use if it is only used by a handful of companies. Providing a standard that many companies build to is the only way to leverage the real benefits of open control networks for whole building control. When hundreds of companies accept a standard network operating system and build their products to the same published interfaces, a market standard is created. This has occurred with the LNS Network Operating System.

In the new open marketplace many manufacturers do not want to create entire control systems. These manufacturers simply wish to produce best in class devices. A standard network operating system like LNS allows the manufacturers of these devices to concentrate on their device and not be concerned about creating an entire control system. This reality combined with the market presence of LNS has caused a proliferation of manufacturers to produce best in class LONWORKS products for use in open systems. These products are the network tools and open devices described below.

3. Standard Network Tools

Network tools include network integration tools as well as HMI application development tools, data loggers, and other applications with a system-wide view. Choosing network tools is easy when following this recipe. Simply look for any tool based upon the network operating system chosen in step 2. The benefit is the use of this tool for either the entire system installation or any portion thereof. It is thus possible to choose any tool for any given project. Tools can be chosen based on functionality and usability rather than who made the physical devices. For network integration tools, be sure to select tools that support the network operating system plug-in standard, that fully support LONMARK objects and configuration properties, and that make it easy to reuse parts of your network design. These features are provided by the LonMaker for Windows Integration Tool, which is the most popular network integration tool for open LONWORKS networks.

4. Standard Device Messaging

It is crucial that the devices installed on the common infrastructure share information without effort. So the forth ingredient in the open system recipe is products adhering to a common communication guideline. As previously determined, this means the devices must use information-based control based on standard functional profiles and network variable types. This is best achieved within the LONWORKS system by choosing LONMARK products.

5. Standard Device Configuration

Recall that according to our definition of an open device, a device must not only support standard communication, it must support a standard interface for configuration. Again, the LONMARK logo on the device is the first place to look. The LONMARK guidelines provide for the physical layer requirements of devices as well as the common functional profiles, data types, configuration capabilities, and installation methodologies.

For simple devices, it may be adequate for product manufacturers to simply document the configuration interface for their device. However, it's obviously better, and required for complex devices, if they encapsulate the knowledge into a plug-in that can be run inside one of the network integration tools. The plug-in must be based on the same network operating system selected in step 2. This allows tools from other manufacturers to install and configure the device quickly and easily.

6. IP Support

The Internet Protocol (IP) suite is the standard on which the Internet is built. An open control system must provide for encapsulation of the control system messages or packets into IP packets. Messages can then be passed around the world without translation into foreign protocols. The cost of transmission is minimal and the ability to leverage existing infrastructure practically limitless. IP support for a LONWORKS network can be provided either by an LNS Server or an i.LON 1000 IP Server that is attached to both the LONWORKS network and the IP network,

7. Gateways – limited to legacy applications

Gateways are the seventh and final ingredient in the open system recipe. This is an ingredient that must be closely monitored. At any point in the system where the messages between devices are mapped from one communication protocol to another, the control network effectively ends. The mapping of messages from one protocol to another is accomplished via a gateway. Gateways should only be used for interfacing to legacy systems or in situations where LONWORKS systems are unavailable. Every other ingredient in the open system recipe can be increased without concern. This is part of the beauty of open systems and the open system recipe. Gateways, however, must be used with great care.

Gateways have been a staple of the commercial control industry for the last 10 years. They are, however, bottlenecks in the flow of system data and are inherently performance limiting. Performing the functions of a gateway requires processing power, which translates into higher cost. Gateways also require someone to indicate what should be mapped to what which consumes engineering efforts. Furthermore, gateways are difficult to maintain. Any change in system parameters has to be addressed at the gateway as well. As a gateway is a transition from one communication protocol to another, it almost always is accompanied by a change in network management schemes. Different management schemes mean different tools are required for either side of the gateway. Therefore, a common network management tool for the entire system is difficult if not impossible to produce. Finally, gateways and their network management tools are closed and proprietary. Since there are no open standards for gateway configuration, the network management tools that address gateway configuration become closed and proprietary, and lock you into a single vendor for the gateways.

7

Implementing Open Systems

This chapter explains the steps required to implement open control systems.

Implementation Tasks

It is important for the specifier to realize that a system integrator performs four major tasks to implement a network control system – system design, network configuration, application configuration, and installation. Each of these tasks requires network integration tools like Echelon's LonMaker for Windows Integration Tool.

System Design

System design consists of two steps: first, selection of LONWORKS devices that incorporate the necessary I/O points — or can interface to legacy I/O points — and that have application programs suitable for implementing the necessary control functions such as PID loops and scheduling.

Second, determination of the appropriate types and numbers of channels and then selection of routers to connect them. This includes a critical decision on the selection of the backbone. Large systems will typically use an IP backbone, medium-sized systems may use an IP or TP/XF-1250 backbone, and small systems may use a TP/FT-10 backbone.

Network Configuration

Network configuration includes the following steps:

- Assigning domain ID and logical addresses to all devices and groups of devices.
- Binding the network variables to create logical connections between devices.
- Configuring the various LONWORKS protocol parameters in each device for the desired features and performance, including channel bit rate, acknowledgement, authentication, and priority service.

Network configuration may be quite complex, but the complexity is hidden by the network integration tools that are part of the LONWORKS system. Functional network design is as simple as dragging the devices' application functional blocks onto a drawing and connecting inputs and outputs to determine how functional blocks communicate with each other.

Network configuration can be either an ad hoc process or a pre-engineered process: in the *ad-hoc* method, the devices are already connected to the network and powered-up, and the configuration data is downloaded over the network as it is defined. In the *engineered* method, the information is collected into a database by the network integration tool and is downloaded to the devices at installation time. In either method, the network integration tool automatically maintains a database that accurately reflects the configuration of each node in the system.

Application Configuration

Application configuration is the process by which the application program in each device is tailored to the desired functionality. Selecting the appropriate configuration properties does this. Each device manufacturer defines how this is accomplished. Most manufacturers provide for downloading the configuration over the network, but a few still require the attachment of a special tool, such as a handheld programmer, directly to the device. The LNS Network Operating System provides a platform for manufacturers to create easy-to-use graphical configuration interfaces, called *plug-ins***,** that are then automatically compatible with any other LNS network tool. For example, the applications in the Echelon LonPoint Modules all have LNS plug-ins for configuration. After defining and performing network configuration of one of these devices using the LonMaker tool, the user can simply right-click on a LonPoint functional block, select Configure from a shortcut menu, and the application plug-in is immediately started from within the LonMaker tool.

Installation

Installation consists of the following:

- Installing the physical communication media for the channels.
- Attaching the LONWORKS devices, including routers, to the channels.
- Attaching legacy I/O points to the LONWORKS devices.
- Using a network integration tool to download the network configuration data and application configuration data to each device, which is known as *commissioning* a device.
- For devices whose application programs are not pre-loaded by the manufacturer, the network tool downloads the application program into non-volatile RAM memory in the device.

Devices are usually either commissioned and tested one at a time or commissioned in off-line mode, then brought on-line and tested one at a time.

Benefits of an Open Implementation

The controls industry has historically provided limited interaction between various control functions. Proprietary architectures have always found a way to preclude leveraging the components of one system for use in another. Non-standard communications and outdated design practices have made providing integrated control costly and difficult.

Open integration allows control applications to leverage all of the investment in control components to integrate formerly disparate systems without difficulty. Such integration increases the flexibility of the control system and its value to the end-user.

No single company can possibly manufacturer best in class components for every aspect of a complex control system such as a building control system, industrial control system, or a transportation control system. Separate manufacturers building components with proprietary communications makes true integration difficult and costly. The only reasonable solution is for manufacturers to build components to a market standard. Consultants must then properly specify these systems to serve their clients' needs.

Appendix A

Glossary

This appendix defines some of the more common terms or phrases used when discussing the LONWORKS system and interoperability.

BACnet – The trademark used to refer to the Building Automation and Control network, which is a protocol communication standard developed by ASHRAE. The 500-page protocol specification indicates how a system's components are configured to share information and work with each other. Currently, BACnet defines 35 message types, divided into five classes.

Certification – A written statement or symbol proving that a product or device meets a certain standard. The certification indicator for LONWORKS products is the LONMARK logo.

Configuration Property – A data value used to configure the application program in a device.

Device – Shorthand name for a LONWORKS device.

Echelon Corporation – The company, headquartered in Palo Alto, California, that invented, sells, and supports the LONWORKS system.

Functional profile – LONMARK specification that enables equipment specifiers to select the functionality they need for a system. Functional profiles define a set of mandatory and optional network variables and configuration properties, along with their intended usage. A small number of functional profiles are available for generic devices such as simple sensor and actuators. Many industry-specific functional profiles are available for industry-specific application. Industry-specific profiles are developed through a review and approval process, including a cross-functional review to ensure the profile will interoperate within an individual subsystem and also provide interoperability with other subsystems in the network.

Gateway – A host computer that connects networks that communicate in different protocols. Gateways are more complex than routers because they handle the conceptual elements involved in allowing one application protocol to work with another. Much of the complexity is visible to the integrator, who must often determine how to translate between the different protocols.

IP – Acronym for Internet protocol, the basic programming foundation that carries computer messages around the globe on the Internet. Sometimes called TCP/IP (Transmission Control Protocol/Internet Protocol), even though TCP is a protocol that runs on top of IP, and IP supports other protocols besides TCP.

Interoperability – The ability of systems from different manufacturers and of different types to share information with each other without losing any of their independent functional capabilities, and without requiring complex programming by the integrator.

LAN – The acronym for local area network. A LAN is a communications network that links a number of different workstations in the same area. The local area may be defined as the same building or campus of buildings. Using the LAN, individual workstations or computers can send messages and files to each other and to shared devices, such as printers, disk storage and other computer systems. LAN performance is measured in the amount of data that can be transmitted and received, usually expressed as megabits transmitted per second, so its critical factor is speed.

LON® – An acronym for local operating network. The difference between a LON and a LAN: LAN is designed to move data that can be long and complicated; a LON is designed to move very short sense and control messages that contain commands and status information to trigger actions. LON performance is measured by the number of transmitted commands and responses. The critical factor in a LON is correct signal transmission and verification.

LONMARK logo – A symbol developed by the LONMARK Interoperability Association that indicates a product can be used in a multi-vendor interoperable system. LONWORKS devices must be certified to carry the LONMARK logo.

LONMARK object – An implementation of a functional profile on a LONWORKS device. A LONMARK object must include all mandatory network variables and configuration properties defined in the functional profile, may include any optional network variables and configuration properties, and may also include manufacturer-specific network variables and configuration properties.

LONTALK protocol – See LONWORKS protocol.

LONWORKS device – Hardware and software that runs an application and communicates with other devices using the LONWORKS protocol. May optionally interface with input/output hardware. Includes at least one processor and a LONWORKS transceiver. Typically includes a Neuron Chip.

LONWORKS network – Intelligent devices that communicate with each other using the LONWORKS protocol over one or more communications channels.

LONWORKS protocol – The open control networking protocol developed by Echelon Corporation. Also known as the EIA 709.1 Control Networking Standard, and as the LonTalk protocol.

LONWORKS system – Echelon's family of hardware and software products that allow customers to develop, build, install, and maintain LONWORKS networks. In total, Echelon offers more than 75 different products for the LONWORKS system.

Network variable – A data item that a particular device application program expects to get from other devices on a network (an *input network variable*) or expects to make available to other devices on a network (an *output network variable*). Examples are a temperature, switch value, and actuator position setting.

Neuron Chip – A microprocessor that is at the heart of most LONWORKS products. Originally designed by Echelon and manufactured and sold by Cypress Semiconductor, Motorola and Toshiba.

Node – Another name for a LONWORKS device.

Peer-to-peer communications – A form of communication where individual network devices can communicate directly with each other, so a central control system is not required.

Protocols – Rules that order how information is transmitted and presented. An “open protocol” is one in which the manufacturer has made the language “translation” available to anyone who wishes to use it.

Router – A device that forwards information from one network or subnetwork to another, based on simple protocol rules. Routers require minimal configuration to enable them to optimize their routing decisions. In normal operations, routers do not store any messages that they route.

SCPT – An acronym for Standard Configuration Property Type. SCPTs are standardized definitions of the units, scaling, encoding, and meaning of the contents of configuration properties.

SNVT – An acronym for Standard Network Variable Type. SNVTs are standardized definitions of the units, scaling, and encoding of the contents of network variables.

Transceiver – A device that is both a transmitter and a receiver for a communications channel.

Appendix B

Frequently Asked Questions

This appendix asks and answers some of the more frequently asked questions concerning the LONWORKS system.

What does the LONWORKS protocol provide?

Protocols today are generally designed to follow the ISO standard *Open Systems Interconnection Reference Model*, which encompasses a full set of protocol features, and classifies them according to seven functional categories (referred to as *layers*). The layers are hierarchical, with layer 1 corresponding to the hardware signalling on the network communications media, and layer 7 corresponding to the application data that is exchanged between network devices. The 7 layers are sometimes called the *seven-layer OSI model*.

The LONWORKS protocol implements all seven layers of the OSI model, and does so using a mixture of hardware and firmware on a silicon chip, thus precluding any possibility of accidental (or intentional!) modification. Features include media access, transaction acknowledgement, and peer-to-peer communication, and more advanced services such as sender authentication, priority transmissions, duplicate message detection, collision avoidance, automatic retries, mixed data rates, client-server support, foreign frame transmission, data type standardization and identification, unicast/multicast/broadcast addressing, mixed media support, and error detection & recovery.

Is the LONWORKS protocol reliable?

The LONWORKS protocol offers two principal reliability techniques. Reliable delivery is assured by true end-to-end acknowledgements (most protocols can only guarantee that a packet was successfully transmitted, not that it was actually received by the application). Data integrity is ensured by the fact that all packet transmissions incorporate a full 16-bit error correction polynomial.

End-to-end acknowledgements are provided using the LONWORKS protocol acknowledged service. This service assures that when a sending device sends a message to a receiving device or devices, that the sending device will get a confirmation that the receiving device or devices received the message. If the confirmation is not received back within a specified time period the sending device will retry to send the message. If after a number of retries the confirmation has still not been received an error message will be logged to the sending device, and the sending device's application will be informed of the error.

Additionally, transceivers for difficult media (i.e., low bandwidth, with high noise and attenuation) incorporate forward error correction data in each packet, able to detect and correct single bit errors without retransmission.

Is network performance predictable? Is a LONWORKS network deterministic?

Most networks that use the carrier-sensed multiple access (CSMA) protocol are non-deterministic because devices are not provided equal access to the network at specified minimum time delays. The LONWORKS protocol adds a unique priority mode to the traditional CSMA protocol that can be deterministic for critical network variables. The CSMA protocol is a listen-before-transmit scheme in which a device with a message to transmit first listens to the network. If no message traffic is detected, then the device will transmit its message after a calculated number of packet time slots. This delay is shorter for priority messages, ensuring that priority messages will be transmitted before non-priority messages, and providing a deterministic upper bound on transmission time. The benefits of the CSMA protocol over deterministic token passing protocols become apparent during high traffic and network overload conditions. The LONWORKS media access protocol uses a predictive p-persistent CSMA protocol, which dynamically adjusts the number of packet time slots, based on predicted network traffic. By dynamically allocating network bandwidth, the predictive p-persistent CSMA protocol permits the network to continue operating in the presence of very high levels of network traffic without slowing the network during periods of light traffic. The benefits of this technology are its deterministic response for priority messages during periods of high network loading, linear response to offered traffic load, consistent performance independent of network size, high efficiency, low overhead, low cost hardware, elimination of the need for network-wide synchronization, and lack of loss-prone tokens.

What are the LONWORKS network size and messaging limitations?

A LONWORKS network domain is a logical collection of devices on one or more channels and is limited to a total of 32,385 devices. Although the LONWORKS protocol does not support communications between domains, application programs may be implemented to forward message packets between two domains. A LONWORKS subnet is a logical collection of up to 127 devices installed on a single segment within a domain (a segment is either a single channel or multiple channels connected by physical repeaters). Up to 255 subnets can be defined within a single domain.

Network domains are used to logically partition transmission media that must be shared by potentially multiple control network applications. Power line and RF media are the most notable examples.

A group is a logical collection of devices within a domain. Unlike subnets, a group is a collection of devices that are grouped together without regard for their physical channel location. The Neuron Chip allows a device to be configured as a member of up to 15 groups. There is a limit of 256 groups per domain. Maximum group size is 64 devices when acknowledged messaging is used, unlimited size for unacknowledged messaging. Groups are an efficient way to optimize network bandwidth for one-to-many network variable and message tag connections.

Network data transmission speed and maximum number of devices per channel is a function of channel type; the speed is 1.25 Mbps for the TP/XF-1250 channel and 78 kbps for the TP/FT-10 channel. Each can support up to 64 devices.

See *LonTalk Protocol* (005-0017-01C) and *LONMARK Layers 1-6 Interoperability Guidelines* (078-0014-01E) for more details.

What is a Neuron Chip and why use it?

The Neuron Chip is actually silicone chip with three 8-bit inline processors in one. Two of the processors execute the LONWORKS protocol, leaving the third for the device's application. It is therefore both a network communications processor and an application processor. Up until recently, all devices on a LONWORKS network required a Neuron Chip.

Having two processors dedicated to network tasks and one dedicated to application tasks ensures that the complexity of the application does not negatively impact network responsiveness and vice versa. Additionally, packaging both functions onto one chip save design and production costs.

Use of the Neuron Chip ensures a controlled hardware execution environment for the protocol. To ensure sufficient processing power, the protocol is implemented with a mixture of hardware and firmware.

The use of a custom chip also allows the inclusion of additional functionality to facilitate control device design. The Neuron Chip incorporates watchdog timers, on-board diagnostics, 35 device controller types, a distributed real-time operating system, run-time libraries, three types of memory, and even a 48-bit software-accessible serial number (which, guaranteed by the chip's manufacturers to be unique, provides an always-available installation address for any Neuron Chip-based device).

Designed for a broad range of industries and applications, and consequently manufactured in volume by two of the world's largest semiconductor manufacturers, the Neuron Chip offers a lower-cost instantiation of the LONWORKS protocol than could be achieved in custom implementations.

The net result is that the Neuron Chip is the best and most economical LONWORKS processor for most LONWORKS devices.

What is interoperability and what are its benefits?

Echelon defines interoperable as the ability to integrate products from multiple vendors into flexible, functional systems without the need to develop custom hardware, software, or tools.

Following are the benefits of interoperability:

- Interoperable products allow project engineers to specify best-of-breed systems rather than be forced into using one vendor's entire line of products.
- Interoperable products increase the overall market for your products by allowing you to compete for what would otherwise be closed bids.
- Interoperability decreases product costs among your business' divisions by allowing your engineering teams to build to a standard specification.
- Interoperable systems allow building, factory, and plant managers to monitor facility-wide using standard tools, regardless of which company made a particular sub-system.

How is product interoperability assured?

For many users of control networks, this is the single most important question. Interoperable products can expand your business, increase your profit margins, save your customers money, and offer you increased vendor choices when specifying systems. In short, it's good for everyone from developers, to integrators, to end-users. Integration without frustration – the ability to integrate products from multiple sources without the need for custom development – can be the driving force that leads to the search for a control network technology.

LONWORKS networks approach interoperability in three ways.

First, up until 1996, Echelon made the protocol available on the Neuron Chip only. Since most every LONWORKS device available today has a Neuron Chip in it, they share a baseline level of interoperability. The Neuron Chip encapsulates as much as possible into standard silicon, to reduce the potential for diverging interpretations. This serves two purposes. One, it provides to every LONWORKS application using Neuron Chips a fundamental commonality at the silicon level. Two, it provides over 10 million (and counting) devices installed worldwide, and each can be thought of as an interoperability reference for any ported processor (non-Neuron processors running the LONWORKS protocol). Echelon ensures, via license, that any port of the protocol must interoperate with the Neuron chip.

Second, it incorporates standard types and objects (so products can agree on the meaning of shared data), and an intrinsic control model (because extrinsic control limits interoperability) into the programming model.

Third, an independent body, the LONMARK Interoperability Association, has been established to manage the evolution of both the interoperability model and the certification of products that conform to the interoperability standard.

The association establishes technical guidelines and promotes the LONMARK interoperability standard worldwide.

What guidelines are followed to achieve LONMARK certification?

All LONMARK-certified devices go through the same certification process. You can get the details from the LONMARK website at ***www.LONMARK.org***. If you have questions about specific devices, or find that specific devices do not comply with the standards, notify the LONMARK Association via the contact link on the web site.

Where can I get information regarding LONMARK product compliance guidelines?

The LONMARK website, www.LONMARK.org, has all applicable documents available for downloading. In general, an integrator will have little need for the information concerning the layer 1-6 information. It is the layer 7 (application layer) information that is most relevant to the network integrator.