Open System Design Guide

Designing Open Building Control Systems Based on LONWORKS® Technology.

Version 2.0

CHAPTER 1: INTRODUCTION

LONWORKS control technology has been experiencing a strong adoption rate in the commercial 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/specifer 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 commercial control projects. Most building automation projects in North America continue to be implemented as multiple, isolated subsystems. Rather than viewed as a whole, building 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 LONWORKS technology 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 LONWORKS technology 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 technology, 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.

LONWORKS technology 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. LONWORKS technology, however, is an enabling platform, not an end-use solution that guarantees seamless interoperability. Use of the LONWORKS technology 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.

This document is provided to assist those interested in designing open control systems using LONWORKS technology. The document provides information regarding the proper design of LONWORKS networks and explains how to leverage the technology to achieve open control networks. It is not intended as a comprehensive reference. The last chapter provides a list of more detailed related reading.

CHAPTER 2: TRADITIONAL SYSTEM ARCHITECTURES

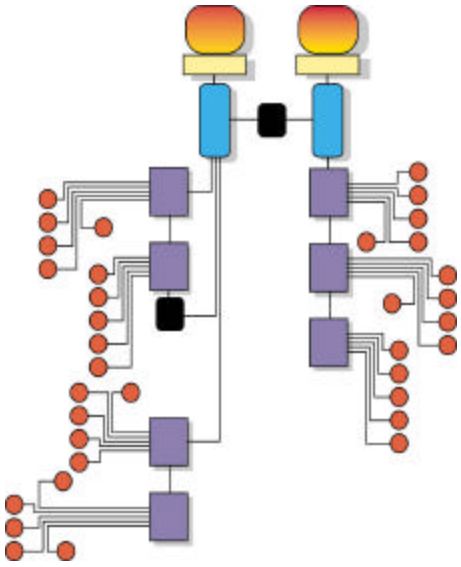
2.1 THE TRADITIONAL APPROACH

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 building. 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 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 can not be shared, information from different sensors is not always accessible, and systems can not adapt their responses in real-time based on the overall system status. It is possible to create intelligent building applications using gateways and custom programs, but they are typically not cost effectiveness and reliability of the systems suffer. Once complete, the owner is forever married to those who provide the gateways and custom programming

The figure to the right 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. 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.



2.2 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, in both building and process control, is as shown in Figure 1. Here we see LONWORKS controllers connected on isolated LonWorks channel segments. The emphasis is still on wiring sensors and actuators back to boxes rather than distributing the intelligence to the field devices. 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.

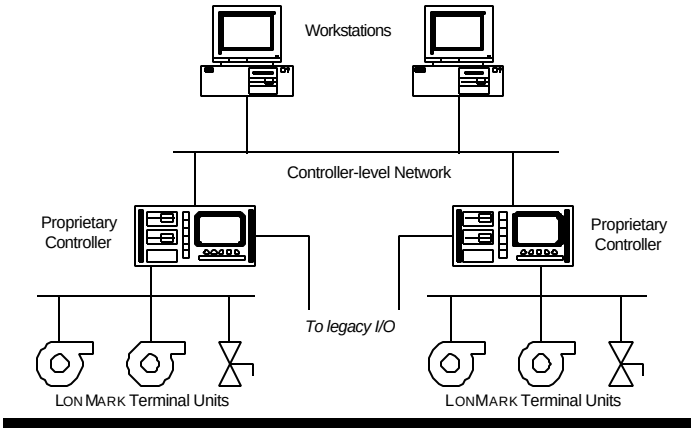


Figure 1. A typical system architecture today

This architecture does not capitalize on all of the power of LONWORKS TECHNOLOGY. LONWORKS nodes in this architecture typically have limited decision-making responsibility and very limited interaction with nodes on other channel segments. 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 supervisor controllers. These devices implement most of the control relationships between I/O devices, terminal units, and and other supervisor 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 one off, custom 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

The architecture shown in figure 1 is not the optimal control solution for a number of reasons. The most important reasons to the end user directly involve life cycle costs:

1. *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.
2. *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.

3. *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.

The system architecture shown in Figure 1 is cumbersome and costly for end-users and systems integrators and it confuses the uninformed buyer who is led to believe he is purchasing an open system because it is based upon a technology that was conceived to provide openness. 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 channel.
Instead of open network management software coordinating information transfer, there is proprietary 'black box' software managing the controller-level network. This software is 'valuable' because it hides the complexity of the two-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 services at some point in the future.

CHAPTER 3: CONTROL NETWORK DESIGN PRINCIPLES

3.1 OPEN SYSTEM DESIGN REQUIREMENTS

The lowest cost and most powerful way to deploy LONWORKS is to build highly distributed peer-to-peer systems. Figure 2 illustrates the logical concept of this approach. The physical implementation may include backbones and routers as required to mediate traffic and provide required performance. Note that 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 support reflect the owner's desire to implement truly open systems.

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

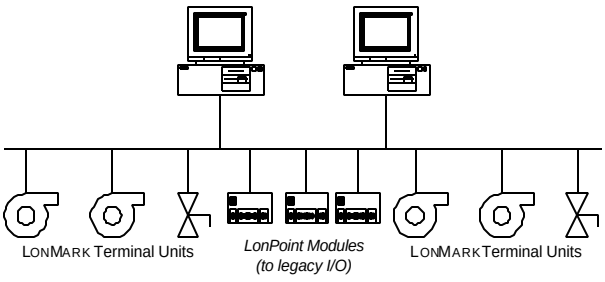


Figure 2. A fully distributed LONWORKS system

Control systems are evolving to truly open, standards-based peer-to-peer architectures in a manner similar to that of the information systems markets. LONWORKS 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 LONWORKS technology and be provided with the proper tools and information regarding products. Recently, a number of new products were introduced that allow consultants to design complete solutions using LONMARK products from multiple vendors. These solutions distribute the control algorithms and legacy I/O interface to the LonWorks device level, eliminating the cost and complexity of 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 powerful software "function blocks" which can be combined to create complex control algorithms.

3.2 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 nodes in the system using the LonTalk communications protocol on whatever physical medium is best (twisted pair, AC power line, radio frequency, fiberoptic cable, infrared). Each node has its own simple application program so that the control logic is distributed throughout the system; the node application is customized by setting configuration parameters rather than by custom programming. In principle, every sensor or actuator in the system can be a LONWORKS node; 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 node.

One of the more popular arguments advanced against the 'flat' 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 the 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 technology 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*. TCP/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 2, 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 TCP/IP instead of proprietary protocols. As shown in Figure 3, the system now uses *tunneling routers* between channel segments, instead of gateways. LONWORKS

messages are 'tunneled' into the TCP/IP packets and sent over the TCP/IP network. 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 envelope, with a different kind of addressing, and the wide-area network delivers this to the addressed remote LONWORKS network segment, where the outside envelope is discarded and the LONWORKS envelope is placed onto the local network segment. 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. This means, for example, that a tool connected anywhere can interact with any node on any segment.

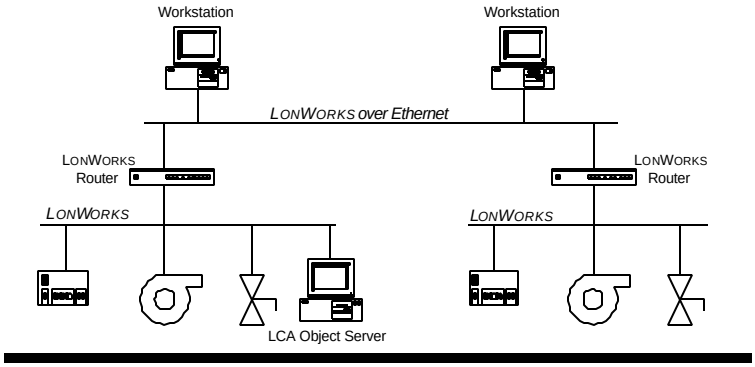


Figure 3. A fully distributed LONWORKS system using an Ethernet backbone

LONWORKS to TCP/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. These devices are already available from a number of vendors and a LONMARK standardization effort is well underway.

An important benefit of this flat 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.

3.3 LEVERAGING INFORMATION BASED CONTROL

The LONWORKS technology makes possible **information-based control systems**, rather than old-style **command-based control systems.** This means that in a LONWORKS system, each node application program 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, nodes issue control commands to other nodes, so a command-issuing node, 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 nodes that can easily be integrated. A major innovation of the LONWORKS technology is the concept of **network** variables**,** which makes it easy for manufacturers to design devices that systems integrators can readily incorporate into interoperable, information-based control systems.

The benefits to an end-user or system integrator of the LONWORKS-enabled "flat" control architecture are:

- A wide variety of compatible, cost-effective LONWORKS devices available from multiple vendors,

- A variety of easy-to-use HMI and network-management 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, and
- Ease of implementing new functions to meet end-user needs.

3.4 BACNET FOR LEGACY NEEDS

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 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 with a system using LONWORKS. 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 nodes. There are cases, however, when the hierarchical system is not needed because the system is completely distributed and the LonWorks nodes 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 a 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 indepth 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 4.

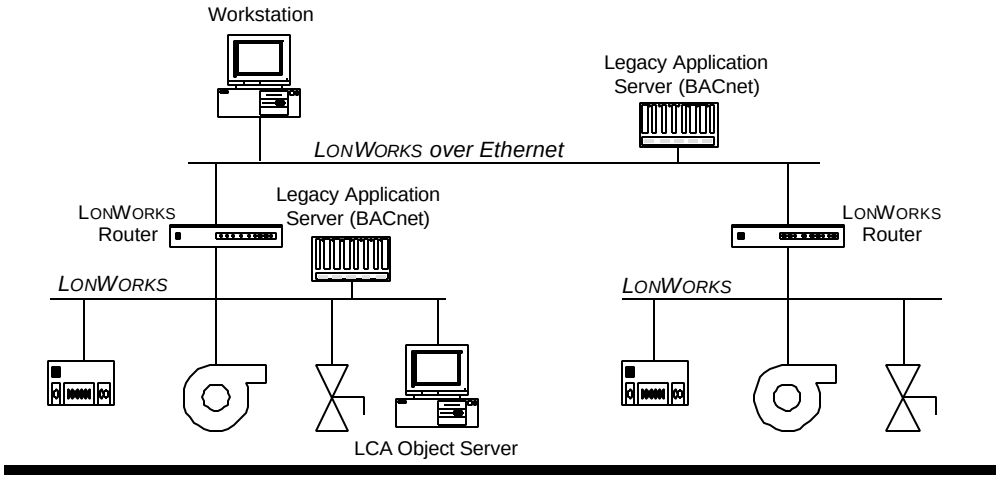


Figure 4. A fully distributed LONWORKS system with an Ethernet backbone using BACnet Servers

In this architecture, subsystems can communicate with legacy systems using BACnet-style servers, just as they do in figure 1. Unlike figure 1, however, there is complete network connectivity as in figure 3. 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. LONWORKS, on the other hand, was designed with the flexibility to meet the requirements of all industries: it 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.

CHAPTER 4: OPEN SYSTEM DESIGN GUIDELINES

4.1 MORE THAN OPEN DEVICES

LonWorks® technology has without doubt played a part in increasing the expectation set for integration and 'openness' in building controls. 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 LonWorks® standard 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 applets or '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.

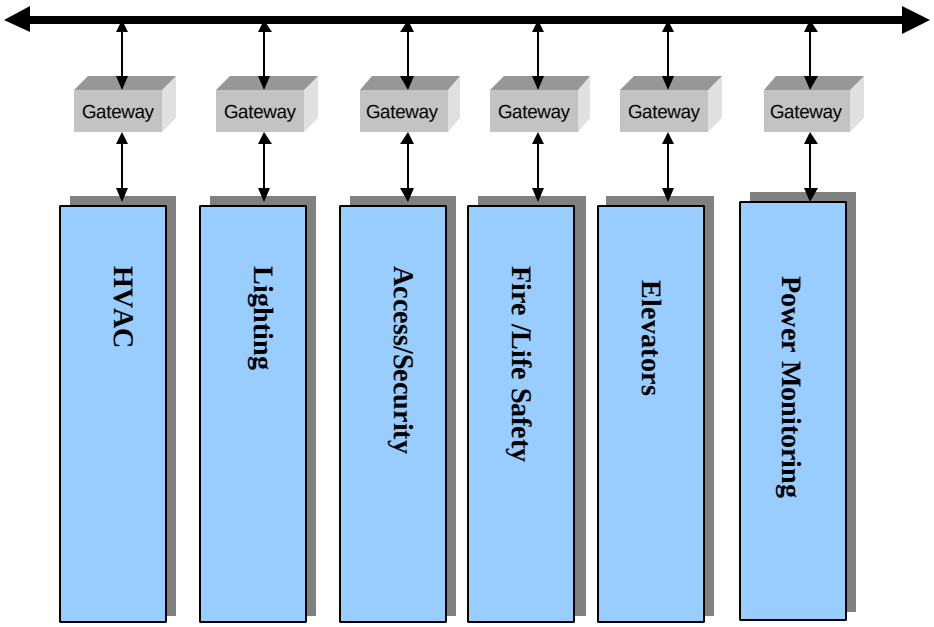
Peer to peer control networks provide measurable advantages over master/slave architectures.

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.

LonWorks technology has become the platform of choice of constructing open systems in the commercial building market.

The traditional control structure in the commercial industry 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 below are the tradition in the commercial control market. 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.



Islands of Automation

4.2 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 building control. Leveraging is achieved by eliminating the walls between building 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 building control.

In this case, the entire building 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 management 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 building-wide open control systems.

1. INTELLIGENT NETWORK WIRING

The base for a building 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 building 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 building functions. This requires the owner and the consultant understand that the building 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 LonWorks Network Services.

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 management tools as well as HMI's, 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.

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 standard communication variables and that is best achieved with LonWorks technology by choosing LonMark products.

5. STANDARD DEVICE CONFIGURATION

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

While it's adequate for product manufacturers' to simply document the configuration interface for their device, it's obviously better if they encapsulate the knowledge into a small program that can be run inside one of the network management tools. This allows tools from other manufacturers to install and configure the device quickly and easily.

6. TCP/IP SUPPORT

The Internet Protocol 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 TCP/IP datagrams. 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.

7. GATEWAYS – LIMITED TO LEGACY APPLICATIONS

The seventh and final ingredient in the open system recipe is gateway. This is an ingredient that must be closely monitored. At any point in the system where the messages between devices is 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. Finally, 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.

CHAPTER 5: OPEN SYSTEM IMPLEMENTATION

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 management tools like Echelon's LonMaker for Windows.

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.

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 LonTalk protocol parameters in each node for the desired features and performance, including channel bit rate, acknowledgement, authentication, priority service, etc.

Network configuration may be quite complex, but the complexity is hidden by the network management tools that are part of the LONWORKS technology platform. Functional network design is as simple as dragging the devices' application function blocks onto the drawing and connecting inputs and outputs to determine which function blocks use what network variables.

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

Application configuration - the process by which the application program in each node is tailored to the desired functionality. Selecting the appropriate configuration parameters does this. Each device manufacturer defines how this is accomplished. Most manufacturers provide for downloading the parameters over the network, but a few still require the attachment of a special tool, such as a handheld programmer, directly to the device. LONWORKS Network Services (LNS) 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-based network tool. For example, the applications in the Echelon LonPoint Modules all have LNS-based plug-ins for configuration. After defining and performing network configuration of one of these devices using LonMaker for Windows, the user can simply right-click on the device icon, select Configure from a pop-up menu, and the application plug-in is immediately launched from within LonMaker.

Installation - consists of: installing the physical communication media for the channels. This involves attaching the LONWORKS devices, including routers, to the channels; attaching legacy I/O points to the devices; and using a network installation 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 contained in ROM, 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.

Summary

The commercial controls industry has historically provided limited interaction between various building 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 building control costly and difficult.

Open integration allows building management applications to leverage all of the investment in control components to perform multi-divisional sequences without difficulty. Such integration of these components increases the flexibility of the building.

No single company can possibly manufacturer best in class components for every aspect of a building 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.

CHAPTER 6: GLOSSARY & REFERENCES

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.

Conformance class - A description of the capabilities of a device for communicating information to other BACnet devices. When comparing two similar devices, a higher BACnet conformance class indicates more features are covered.

Functional group - Basically, a BACnet term used to describe collections of BACnet features that are required to accomplish certain common functions, such as alarm reporting or file transfer.

Native BACnet. When the BACnet communication protocol is interpreted and implemented in a specifi product by the manufacturer, it is said to be "native BACnet." In theory, native BACnet products can communicate with other manufacturer's products without a gateway, but a conformance standard does not exist and current products do not provide this feature..

PICS. Acronym for Protocol Implementation Conformance Statement. Created by the manufacturer of a BACnet device, the statement details the BACnet options implemented in the device, including its conformance class, the functional groups supported and a number of other BACnet standard implementation aspects.

REFERENCES

The documents listed below are available from at www.echelon.com or www.LONMARK.org.

1. LONWORKS Technology Overview
2. LONMARK Interoperability Overview
3. LONMARK Layer 1-6 Interoperability Guidelines (078-0014-01)
4. LONMARK Application Layer Interoperability Guidelines (078-0120-01)
5. The SCPT Master List (005-0028-01)
6. The SNVT Master List and Programmer's Guide (005-0027-01)
7. LonManager® Protocol Analyzer User's Guide (078-0121-01)