BACnet 1 2 3

The ASHRAE-devised communications protocol is undergoing more specifier-friendly changes, but in the meantime GSA's guide is a useful tool in specifying systems using BACnet

By Eugene DeJoannis, P.E., Technical Associate, van Zelm Heywood & Shadford, West Hartford, Conn.
Consulting-Specifying Engineer -- 9/1/01

Most consulting engineers know that BACnet is a communications protocol developed by ASHRAE to allow the integration of all types of digital building controllers into a unified system. What many consulting engineers are unaware of is how exactly to specify it.

Indeed, it is readily apparent that the 500-page standard is not very helpful for building-automation system (BAS) specifiers, but rather is more of a guide for equipment manufacturers.

While the fundamental ideas are not hard to grasp, the standard's detailed descriptions are steeped in terms of data structures and object-oriented programming only comprehensible to those fluent in IT jargon. And even if one is able to understand the language, it's still mainly useful to those who make interoperable controllers, as it defines software standards necessary to build system databases, including how to construct a BACnet message that conveys data about a device in the system.

The good news is that the standard is under continuous maintenance and now boasts several large addenda, with more in the pipeline. The bad news is that there is still little guidance on how to specify a BACnet control system. One resource available, however, is a guideline produced by the U.S. General Services Administration, "GSA Guide to Specifying Interoperable Building Automation and Control Systems Using ANSI/ASHRAE Standard 135-1995, BACnet," available at http://www.bacnet.org/. The following delves into the guide's recommendations.

Breaking down BACnet speak

The basic idea behind BACnet when it was first implemented was to create a set of simple data structures called "objects" that could be assembled as needed, to describe any direct-digital controller (DDC) in the system software. Objects in BACnet are the very kinds of data that DDC systems have long used.

In specifying typical digital controls, the task falls into two areas: the boilerplate—those specs describing the more general features of a control system—and the detailed parts crafted for a specific job. The latter are the sequences of control for each system and an explicit description of all the points to be controlled. Sequences and point diagrams for a BACnet specification would be identical to one's current practice. Because BACnet has no impact on the logic that will apply to controlling each system, this information is not included in the system-specific part of the specification.

But the boilerplate specs are a different matter. Wherever the specification refers to networks, modems, workstations and data to be exchanged with other control systems—chillers, boilers, fire alarms, variable-frequency drives, lighting—it is necessary to use some new terminology to explain the design.

The "object" is a good place to start. Some objects are familiar, like control *points*—analog or binary inputs and outputs—but other BACnet objects include *calculated values, schedules, event definitions, calendars, commands, device and file descriptions, control loops, programs, trend logs* and the like. By creating a standard description of each object, a controller built up from simple data objects can read the data in "foreign" controllers—devices produced by other vendors—that are also built from simple BACnet objects. Similarly, a workstation can automatically add new devices to the system database as the devices are added to the network.

BACnet objects simplify intersystem communication because the data inside each object describes, in a standard format, the properties of that object. An object's properties—its name and type, or the present value of an analog value object—can be changed by another external BACnet device by sending a specific BACnet command, called a WriteProperty message, to the object's address. The object can also be polled by sending a similar command known as a ReadProperty message.

BACnet objects construct the database describing all the controllers in a BAS system. By discovering what objects are in a new controller and knowing how the data properties are arranged inside each object type, the information becomes addressable and accessible to all BACnet devices in the BACnet inter-network. Thus the standard serves equipment designers as a *dictionary* and *grammar manual* for "BACnet-speak."

There are a limited number of "primitive" objects in BACnet, but they can be assembled, as needed, to construct a software model of any controller, just the way the limited letters of the alphabet can be assembled into an endless variety of words, sentences and paragraphs. If needed, a vendor can add proprietary objects and properties.

BACnet does not restrict how controllers are connected into networks. It allows for several network-wiring types and communication schemes (mostly invented elsewhere), ranging in order of decreasing speed—and decreasing cost—from Ethernet to ARCNET, LonTalk and MS-TP (master/slave-token/passing using RS-485 wiring), to PTP (point-to-point, RS-232) wiring for *remote modem* tie-ins. There can be one network or several networks with multiple levels and data-transfer speeds.

Additionally, there are two methods for sending BACnet messages over the Internet to build wide-area networks. In short, many options are offered allowing the specifier to choose the least costly solution that is fast enough for the volume of data traffic at each BAS network level. *The designer should not specify network type, unless it needs to be compatible with other network investments already in place.* Let the vendors pick the network types in order to avoid unnecessarily limiting the vendors who can compete, because not all vendors offer all network types.

Making the most of a network

In the past, BAS installers have typically put in their own network wiring, which constituted a large percentage of the system's cost. This need not be the case today, as BACnet makes it possible to tie together workstations and building controllers on a business' backbone Ethernet network. The owner, of course, must be consulted, but testing has proven that BAS traffic adds no significant load to other business-related network uses. Lower speed networks for field controllers will likely still be dedicated to the BAS (ARCNET, LonTalk or MS-TP). If given the go-ahead by the owner, the specifier should clearly define the type of network provided by the owner and where the connection will be. Section 6 of the GSA guide addresses this topic, and explains that within each network option there are choices of speed, wiring layout and wire media. But unless the project has specific network requirements that the BAS must comply with, vendors can make these decisions.

Inter-network connections

Connecting these networks is a simple matter of joining networks with a standard BACnet device called a *router,* that converts a BACnet message from one communications media to another. It does not change the message format, and except for checking the address to see if the message should be passed through, it does not even look at the contents.

The second function of a router is to filter out messages not addressed to the other side of the router. These devices are the means of connecting the sub-nets that use different wiring media. They can be stand-alone components, but are typically part of high-level global controllers that interconnect low- and high-speed networks. An example of such an inter-network is a low-speed MS-TP that joins the

controllers of an air-handling unit (AHU) and terminal unit to a building's Ethernet network on which the BAS workstations reside. The router for this inter-network connection will usually be part of a BACnet Building Controller (BBC).

In BAS systems that do not use an open communications protocol like BACnet, the system vendor installs the proprietary networks offered by the supplier, and specifying engineers do not get involved in those choices. To assure interoperability between suppliers, it is a must to adhere to standard network types and message formats. If this is not possible, translating computers, known as *gateways,* are used. Unlike simple routers, gateways must inspect the contents of each message and translate it into a format understandable to the connecting networks. The problem with gateways is that they introduce speed and translation problems.

Specifying interoperability

To create an integrated control system, in which components provided by different vendors can interoperate, five general I/O areas must be specified:

- Data sharing
- Alarm or event management
- Scheduling
- Trending
- Device and network management

The first and last items may not be specifically addressed in a standard specification. This is where the GSA guide may help. The most recent updates added to BACnet this past June through *Addendum d* involve the creation of sorely needed data-exchange functions in each of these interoperability areas. They are called *BACnet interoperability building blocks* (BIBBs) and are collections of BACnet services needed to interoperate in these five areas (see "BACnet Unraveled," p. 50, August 2001).

With this in mind, important, soon-to-be standardized BACnet devices include: the operator workstation, the building controller, the advanced application controller (AHU or system controller) and the application specific controller (i.e., terminal unit controller). By referring to these devices in the GSA guide, or *Addendum d* to the standard, a specifier can be assured of a component for each level of a typical BAS with a minimum standard set of features. This will be the basis of the BACnet BAS. Until the addendum is formally issued, specifiers can download the version in the GSA guide and include it directly in the specification (Annexes A & B).

Making it work

Although the arcane terminology within the BACnet standard may be confusing, it is mostly not the specifying engineer's concern. It is enough to read the various articles and tutorials describing BACnet to become familiar with the concepts; the details are for BAS manufacturers to puzzle over.

The new standard BACnet devices and their minimum required BIBBs can be used to describe the outline of a BAS very much like the ones that have been specified in the past.

What is important to spell out are the standard services and the five I/O and calculated value objects. Additionally, the building controller should support the calendar, schedule, loop, trend log and event enrollment objects. Lower level controllers should support the minimum services in their profiles and the loop object in addition to the basic six I/O objects and the calculated value objects.

The BACnet Manufacturers Association will begin certification testing later this year to give specifiers assurance that certified hardware will interoperate.

One final note. Bear in mind that if several vendors will be involved in assembling the BAS, it is important to clearly explain the network layout and responsibilities of each. Also sit down with the owner and define a standard naming and network numbering scheme.

For those who still need additional help, ASHRAE offers a professional development seminar conducted in various cities across the country.

Service Command Priorities Priority Level	Application	Priority Level	Application
1	Manual Life Safety	9	Available
2	Automatic Life Safety	10	Available
3	Available	11	Available
4	Available	12	Available
5	Critical Equipment Control	13	Available
6	Minimum On/Off	14	Available
7	Available	15	Available
8	Manual Operator	16	Available

Speak the Same Language: BACnet Do's and Don'ts

GSA's guide to specifying BACnet hits on a number of other important areas. For example, *object naming* is the subject of section 4. There, readers are advised on how to set up a standard point-naming scheme. Such schemes are not unique to BACnet, and normally a BAS vendor will set up point names as part of the design process. But occasionally the vendor-chosen scheme will not be one the owner likes. In such instances, especially if several vendors will be working on a job, it is critical to establish a common method. The GSA guide recommends a popular system known as FSP. The system employs a format that codes M/E/P systems and devices along these lines: FACILITY.SYSTEM.POINT, as in BLDG20.AHU4.SA_TEMP. If this is the best way to proceed, establish a set of abbreviations for common building equipment so that all vendors use the same language—AHU1, HX1, P1, for example.

Section 4 additionally addresses object properties, such as loop tuning, calendars and schedules, that should be adjustable via the BACnet workstation as opposed to a proprietary software tool.

Section 5 of the guide deals with another important group of concepts: the BACnet services, i.e. messages, wherein object properties can be manipulated, for example, to command a change in setpoint. One can assign a priority level to messages so that the most important ones will override all others. The highest priority of BACnet service commands is reserved for manual life safety. Priority levels 3, 4, 7 and 9 through 16 are unassigned and available for use (see Table). This could be useful when attempting to clearly define which commands take precedence for a BAS that integrates several different types of digital building systems.

Alarms may also be prioritized. In general, BACnet allows 256 levels of alarm priorities. BACnet alarms include a priority value, but it is up to the specifier to make use of it to define the BAS reaction.

In addition, alarms can be assigned a *notification class* number so the system knows who should receive it depending on alarm type, day or time. A custom message text can be assigned to an event to remind the operator of things he or she should check when that event occurs.

As far as monitoring other significant changes of values (COV), there are two ways to do so other than

the BACnet devices asking other devices periodically. The first method is to have the workstation "subscribe" to a COV from other BACnet devices, if the workstation software has this feature. The second method involves data intended to be shared by all controllers. In these instances, another COV service is available that does not require each device to be a subscriber.

Internet Connections

The original ASHRAE/ ANSI standard 135 allows wide-area networking via the Internet using what is called a BACnet tunneling router (BTR). It is inexpensive and the BACnet controllers do not need the hardware and software to communicate in Internet Protocol (IP). Instead the BTR on each BACnet network keeps a list of all the other BTRs in the other remote networks and takes care of readdressing outgoing BACnet messages for their Internet journey. Unfortunately, it involves a bit of manual maintenance work to keep these lists up-to-date, but existing networks with controllers that cannot handle IP messages directly will have to use this method.

The newer BACnet/IP requires that all the individual controllers on a network are able to use IP messaging, and they can send their messages to specific controllers on a remote network. However, this doesn't always work for broadcast messages (to all recipients), because IP routers usually filter out such messages. By adding a BACnet broadcast management device on each sub-net, a broadcast message can be sent directly from one BBMD (BACnet Building Management Device) to the other, and then rebroadcast on the receiving network after it passes the IP router that provides the Internet connection. Several native BACnet vendors have recently added a new choice to consider: instead of putting their BAS database software for a building on a BACnet workstation, it's placed on an Internet server. In this arrangement, anyone with a password and a computer with an Internet browser can view the graphical BAS database from a remote location, without investing in workstation software.

Can BACnet and LonTalk Work Together?

One obvious question many specifiers ask is whether BACnet and LonTalk can work together? The answer is yes. The GSA guide features a short discussion of the LonTalk network design and LonWorks or LonMark controllers. The important thing to realize is that LonMark controllers will not interoperate with BACnet networks without the addition of a gateway. LonWorks controllers use the LonTalk network. This may be a bit confusing because BACnet allows LonTalk as one of its four network options. However, the message formats of each system are completely different, so the different controllers will not understand the other controller type.

Additionally, some BAS manufacturers have developed a line of LonWorks or LonMark controllers, but no BACnet vendors have chosen to use LonTalk technology for their field controller networks. Those who have all BACnet product lines have used ARCNET or MS-TP for these networks.

If a modem connection to the telephone network is desired, the PTP protocol should be specified and the optional password protection should be included. The two modems connected by telephone lines will behave like a router between the BACnet networks for the call duration.

Managing BACnet Addresses

If BACnet is being used to monitor multiple buildings, it is necessary to develop an addressing scheme with the owner. Each device address must be unique. Addresses consist of a network number (up to 65,535) and a device media access control (MAC) address. Device MAC addresses can be the same, as long as they are in different networks. Ethernet and LonTalk chips have embedded addresses when they are made, though the latter may use other schemes. For ARCNET and MS-TP networks (up to 255 devices per network number), the specifier should require vendors to obtain address assignments from the owner if there is any chance that several vendors are connecting devices to the same network and could repeat addresses. In any case, future management of the inter-network will be made simpler if some logical address scheme is used for all buildings. Similarly, the device object identification property must be managed uniformly by the owner of a large system; no duplication is permitted in the same

network domain.