THE OHIO STATE UNIVERSITY Physical Facilities
Partners in Academic Excellence

BACnet Goes To College

Ohio State's Evans Chemistry Lab.

By Jonathan P. Fulton,
Associate Member ASHRAE

As early as 1995, The Building Automation Group at The Ohio State University (OSU) envisioned the integration of multiple building automation systems (BAS) using an open protocol. At the time, the university had hundreds of installations with proprietary systems in 258 buildings (totaling 11.9 million ft^2 [1.1 million m^2]).

In late 1999, the university began working with a controls firm regarding the installation of a native BACnet system. Native systems can be identified as systems that encompass the BACnet protocol throughout their architecture, which possess BACnet objects in all levels of control and do not require the use of gateways or proprietary devices. The goal for this project was to develop a global solution that promoted unity for the university's large campus.

Testing schemes were developed for a native BACnet solution involving leading BACnet system manufacturers. These schemes included various tests on interoperability, networking and database execution. The initial tests were strictly focused on interoperability requiring submission of products from each manufacturer.

Products from each manufacturer were located on two separate LANs and interconnected through the Internet. This setup permitted remote and on-site testing of each system. *Figure 2* depicts the test network architecture for a native BACnet system.

Interoperability Testing

Interoperability testing involved the dynamic creation, deletion and sharing of standard object types in system and unitary level devices (Ethernet, MS/TP and ARCNET). All object types were tested for dynamic creation and deletion. Tests were conducted in a fashion that permitted each vendor's system to execute the mentioned criteria while concurrently connected to the OSU WAN (Internet).

The results, as identified by VTS 3.1.5 (*Figure 1*) and the respective operator workstations (OWSs), indicated the strengths and weaknesses of each product and the restrictions thereof. After several weeks of successful testing, the network performance/security test was scheduled.

The use of BACnet/IP (Annex J) was preferred, as the university has several hundred buildings with connectivity on a public WAN (Internet). Annex H.3 was not considered due to limitations with

remote connections and PAD (Packet Assembler -Dissembler) table updates. (For example, devices are not easily added or removed; the table of peer PAD devices must be changed in every PAD when the configuration changes.[1])

Initially, the use of User Datagram Protocol/Internet Protocol (UDP/IP) was a concern of the OSU IT staff, as "open broadcasting" is not preferred. Unlike TCP/IP (Transmission Control Protocol/Internet Protocol), UDP/IP does not guarantee delivery of data and offers few error recovery services. Fortunately, BACnet guarantees delivery for the critical network services. UDP/IP is a simple and efficient protocol that sends and receives datagrams over an IP network through specific ports. The BACnet committee chose UDP/IP as it supports broadcast messages. However, experience has shown that in large networks, UDP/IP broadcasts can overwhelm devices because every receiving device processes every broadcast message.[1]

For these reasons, the controls firm proposed the use of combination BACnet broadcast management devices (BBMDs)/routers. With these devices, the main campus-wide BACnet/IP network was separated from the local building-wide BACnet networks. The broadcast traffic management would rely on the segmentation of the OSU BAS network and the BBMD/routers for restricting and routing broadcast data from their respective networks to other BACnet networks.

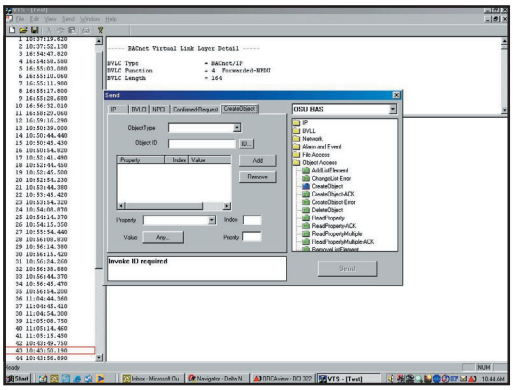

Figure 1: Results of testing native BACnet products using VTS 3.1.5.

Stability of the products was the second, but equally important, concern. Devices had to work under heavy traffic conditions with little or no vulnerabilities. The request and receipt of all data, monitored by a third-party network program, was successful under exceedingly high traffic conditions. This third-party program captured and decoded the data on the network and presented it in a user-friendly format for detailed analysis.

The last and final stage of the BBMD evaluation was an automated vulnerability test (port scan) executed by an open-source utility for network exploration or security auditing. The purpose of the port scan was to eliminate the concern of standard IT attacks, not necessarily BACnet-related attacks.

The port scanner uses raw IP packets in novel ways to determine what hosts are available on the network, what services (ports) they are offering, what operating system (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.[2] The scan indicated that no open ports were found (1,519 total) and displayed each device's OS as an ambiguous platform. All network security/stability experiments endured the rigorous testing of the university and the controls firm.

Database testing included the monitoring of custom programs, time synchronization and events (alarms). The network architecture (public WAN) fueled con-

Ronald Sharpe and Jonathan Fulton developed a BACnet system for Ohio State.

cerns of database corruption. These concerns were addressed by adequately testing each of the aforementioned areas after warm/cold reboots and during normal operation.

Event (alarm) testing consisted of notification class monitoring and creation of simulated alarms. These alarms were acknowledged and/or deleted independently at each OWS. Time synchronization was tested from each OWS and verified at each device.

Programs and I/O scan rates were monitored during each test and while intentionally attempting to sabotage the network through deliberately initiating continuous ping commands simultaneously with the previously mentioned port scan. In efforts to "halt" the systems, further testing included loading repetitive programs to decrease the processor response times. The results were observed and errors were recorded during each phase. With minimal errors, the testing was complete and the installation of a "live" native BACnet system was scheduled.

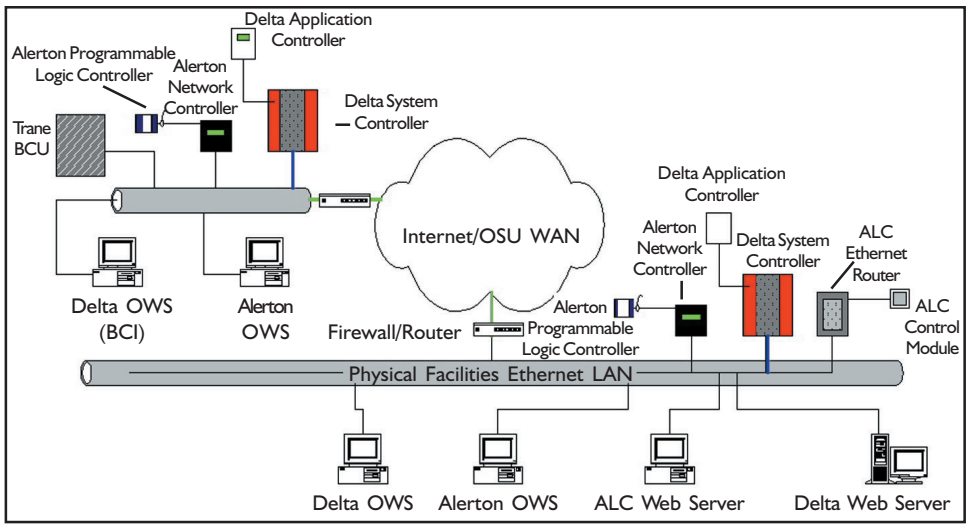

Figure 2: Ohio State test network architecture for a native BACnet system.

Implementation

The decision was made to install the first native BACnet system in the Evans Chemistry Lab. The architecture incorporated three system controllers for control of the main HVAC systems and one operator workstation. The project also included integration with the other principal OWSs. Upon completion, the project was deemed successful and plans were developed for the installation of additional native BACnet systems.

Results

Since the Evans Chemistry Lab project, native BACnet systems have been installed in 10 buildings totaling 679,000ft^2 (63 000 m^2). These buildings are composed of main system HVAC controls and more than 800 I/O points. The BACnet interest has also been adopted by The Ohio State University Medical Center, where installations are underway. The long-term vision is to incorporate the BACnet protocol in all HVAC systems.

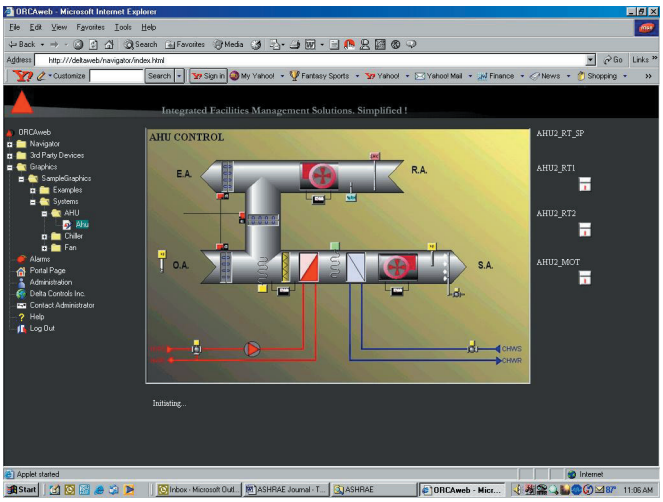

Figure 3: A web browser is used to access the HVAC system.

The direct security measures for BACnet are still in their infancy stages, and require external measures to ensure protection. For this reason, the controls firm has converted the Physical Facilities and Medical Center systems to virtual private networks (VPNs) with limited access. Strategically located firewalls secure the VPNs from unwanted traffic. The Web-servers support secure socket layers (SSL) and only receive port 80 or HTTP traffic. As an extra precaution, the Windows® 2000 Professional platforms were configured to eliminate drive sharing and guest privileges. The APC series battery backups are TCP/IP and SMTP (simple mail transfer protocol) configured, allowing constant monitoring and notification of precarious electrical conditions.

Both servers permit and welcome Internet Explorer and Netscape Navigator clients and the Web-server at Physical Facilities incorporates the data from three other manufacturers. The implementation of the Web server eliminates use of proprietary software and promotes use of external real-time monitoring from practically anywhere. *Figure 3* is a screen capture using Microsoft Internet Explorer 6 to access graphics at OSU.

Future

OSU intends to expand the system to include native BACnet access control,

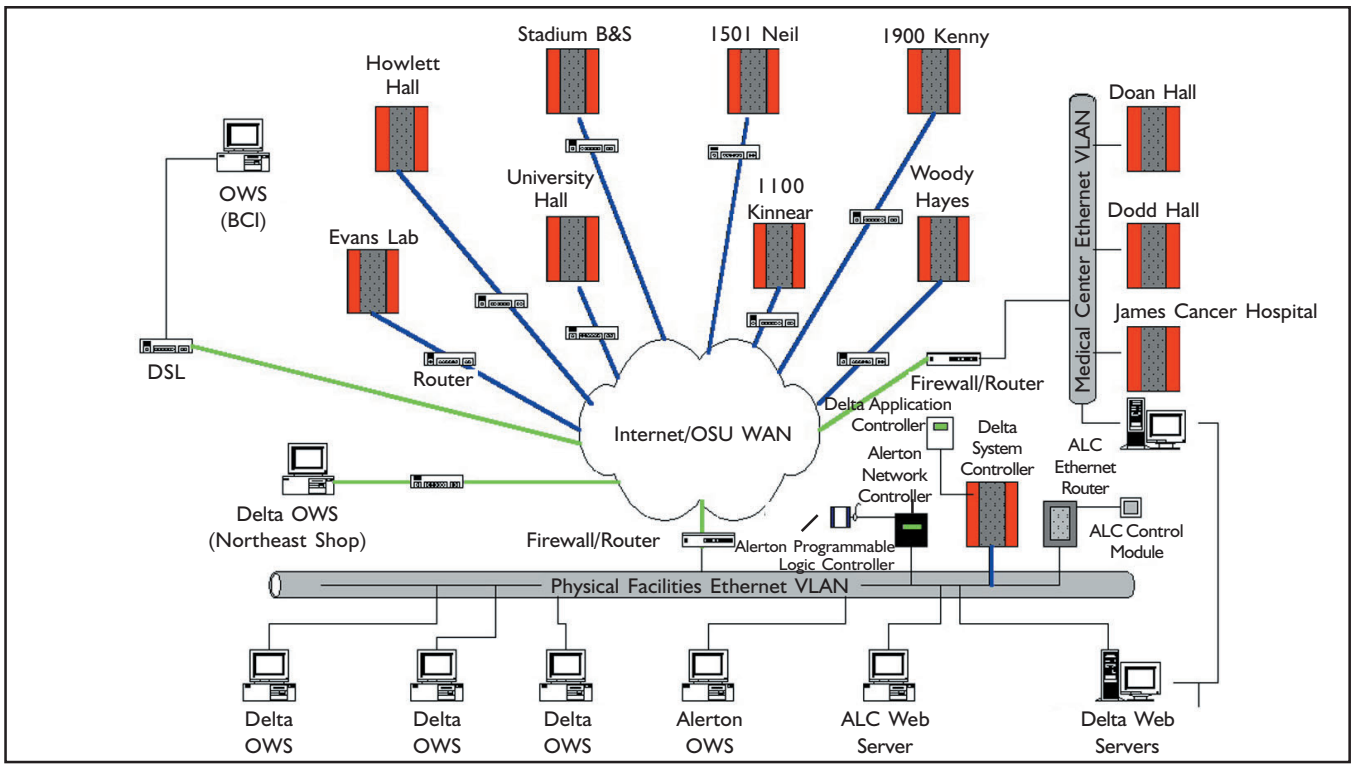

Figure 4: Ohio State's current network architecture. The blue network segments denote BACnet/IP (Annex J) connections as BACnet BBMD. The green network segments indicate TCP/IP connections.

lighting, fire alarm and other related products. Currently, the installation of an access control system is scheduled for completion by Fall 2002. The pilot project will be implemented in the Physical Facilities, Building Automation Shop, and will undergo the same rigorous testing as previously mentioned. Further plans include the development of a standard specification for all building systems (HVAC, fume hood, fire alarm, access and lighting controls).

Moving forward, OSU will focus on standardization, quality assurance and the full implementation of a VPN. The standardization will include a variety of efforts. The intention is to develop a network and product standard. Network standards will specify such items as switches, rather than hubs; automatic network addressing (ANA), peer-to-peer communications, and BACnet/IP with firewall support.

ANA is a method for organizing and configuring devices on a network segment. It provides a manageable representation of the relationships between the devices on a given network. Peer-to-peer communications is simply identified as direct exchanges of data from one device to another, even if the network segments are different. Moreover, peer-to-peer devices have the ability to initiate a request for data. Product standards will be established to classify the required device profiles (BACnet Annex L) and installation methods.

Quality assurance will include continuous independent BACnet testing and benchmarking. The independent test's format will be similar to the test outline in this article and conducted on a semi-annual basis. Collectively, these standards will require BACnet conformance and promote interoperability throughout the university.

Summary

The success at The Ohio State University is the result of detailed planning, testing and strategic partnerships. The installations at OSU are prime examples of the benefits derived from the evolution in control's technology and the explosion of BACnet. The combination of the Information Technology (IT) and Building Automation worlds is powerful. It has worked for Ohio State. "It's our responsibility to find and adopt new ways of doing business…BACnet has allowed us to establish a new standard with a predictable outcome," said Ronald Sharpe, manager of the Building Automation Group at Ohio State.

References

1. Swan, B. 2002. "Building wide-area networks with BACnet." *Engineered Systems.*

2. Nmap Introduction. 2002. www.insecure.org/nmap/index.html.

Jonathan P. Fulton is president of Building Control Integrators, Hilliard, Ohio.