Access Control In BACnet®

By David Ritter; Bernhard Isler; Hans-Joachim Mundt; and **Stephen Treado, Ph.D., P.E.,** Member ASHRAE

The BACnet® standard is extending its scope to incorporate physical access control systems (PACS) and, soon, closed-circuit television (CCTV) control and an interface to logical access control. This extension into the realm of physical security takes BACnet beyond its original scope of HVAC control. With the recent additions of fire detection, energy consumption management and the upcoming lighting control, BACnet has emerged as one of the worldwide building automation and control standards.

Currently, the physical access control industry has no established open standards. In fact, the physical access control industry is in the same state as the HVAC industry was when BACnet was conceived, with physical access controls systems dominated by proprietary solutions, which lock in the customer to the manufacturer. Standardization empowers end users because it allows the system to be built using the best solutions for the application. Within the physical access control industry, this is a concept that is long overdue.

Why is BACnet the right standard for physical access control? First, BACnet has the distinction of being a truly international standard as it is recognized by both the American National Standards Institute (ANSI/ASHRAE Standard 135-2004, *BACnet®—A Data Communication Protocol for Building Automation and Control Networks*) and the International Organization for Standardization (ISO 16484-5, *Building Automation and Control Systems—Part 5: Data Communication Protocol*). BACnet undergoes continuous maintenance by a broad cross section of stakeholders, including manufacturers, specifiers and end-users, which represent the HVAC, fire, physical security, lighting, IT and other building control industries. From the beginning, BACnet was designed to be extensible and adaptable to new applications by providing a comprehensive framework of objects and services. The BACnet exten-

About the Authors

David Ritter is senior software developer/technical lead for Access Control Products, Delta Controls in Surrey, BC, Canada. **Bernhard Isler** is senior system architect, Fire Safety and Security Products with Siemens Building Technologies, Zug, Switzerland. **Hans-Joachim Mundt** is head of standards, Siemens Building Technologies, Karlsruhe, Germany. **Stephen Treado, Ph.D., P.E.,** is mechanical engineer, Building and Fire Research Laboratory with the National Institute of Standards and Technology, Gaithersburg, Md.

With the convergence of building control functions, many facility managers, who have a previously installed BACnet system, find they have inherited the responsibility for physical security or need a package that seamlessly integrates physical security with the rest of the building automation system.

sions for physical access control are built upon this foundation and meet all the requirements for security applications.

With the convergence of building control functions, many facility managers, who have a previously installed BACnet system, find they have inherited the responsibility for physical security or need a package that seamlessly integrates physical security with the rest of the building automation system. BACnet provides the solution to both of these problems.

The power of BACnet is in its ability to interoperate among different vendors and integrate with different building control applications. BACnet provides a universal gateway, through a standardized interface, to and from other enterprise information management systems such as IT, identity management systems (IDMS), human resources (HR), etc. In short, BACnet provides enhanced facility functionality from a single seat of control, providing the benefits of reduced infrastructure and operating costs while improving performance. The benefits seen in the HVAC industry are being realized in the physical access control industry through BACnet.

Introduction to Physical Access Control

The primary purpose of a physical access control system (PACS) is to secure access-controlled zones by restricting access to zones to only those persons (or assets) who are allowed access.

Zones, Doors and Credential Readers

Typically, access-controlled zones are enclosed geographic areas, which may represent complete buildings, specific areas of a building, floors of a building, hallways, stairwells, elevator cars, etc. In some systems the outside of a building may also be considered an access control zone.

The geographic zone is defined by the collection of access points into the zone (ingress points) and out of the zone (egress points). Ingress and egress points typically are doors but may also be gates, turnstiles, motorized doors or other mechanical device depending on the specific application. Access to and from the access zone is controlled through the doors that make up the zone.

An access-controlled door is not a single entity but a collection of door hardware that typically includes controlled outputs, such as a door lock, door holder, door sounders etc., and supervised inputs, such as door contacts, request-to-exit inputs, motion detectors, etc. Access controlled doors typically are locked. However, they may be scheduled to be unlocked during certain times of the day. The door lock may also be controlled by other building automation systems such as the fire detection system or the intrusion detection system.

A person requesting access to an access zone through a particular door presents their access credential at the credential reader. The value read at the credential reader is the authentication fac-

tor. The authentication factor is passed to the PACS, where the determination of whether to allow or deny access is made. Based on this determination, the door may be controlled by the PACS to unlock, allowing the person to enter the secured zone.

A typical physical door configuration is shown in *Figure 1*.

Authentication and Authorization

The role of a PACS essentially is to answer the question of who/what, where, when and why access to a physical area is allowed.

- **Who/What:** What person (who) or asset (what) is requesting access to the access zone?
- **Where:** What zone or door is the person requesting access to?
- **When:** At what time is the person requesting access to this door?
- **Why:** Does the person have permission to access this door?

These questions are encapsulated in a two-step process that consists of authentication and authorization.

Authentication is the process of verifying the identity of the person requesting access through an access-controlled door. This may be as simple as a single-factor authentication, in which one authentication factor (i.e., magnetic-stripe card, proximity-card, smart card, etc.) is used to identify a known user within the access control database in the PACS. In multifactor authentication, a combination of two or more authentication factors (i.e., card + PIN, card + biometric, etc.) are used to verify the identity of the person requesting access. Multifactor authentication provides a higher degree of security and is used in situations where security is a primary concern.

Authorization is the process of determining whether the person is permitted to access the zone that they have requested to enter. Once the person has been authenticated successfully, the PACS checks a list of criteria to determine whether access can be granted. Generally, many authorization criteria must be met before access can be granted. For example, the person must have access to the zone or door at the requested time, the credential used must not be lost, stolen or otherwise disabled, a passback violation must not be in effect, etc. If any of the authorization criteria fail, then the person is denied access. It is only after all the authorization criteria are met that the person will be granted access. Once the person is granted access, the PACS will unlock the door and the person can access the zone.

Event Reporting

Another primary function of any PACS is event reporting. In access control, all events that occur are logged and sent to the host system to be archived. The PACS may report and log the following types of events:

- Access transaction events (e.g., access granted or denied);
- Change of states (e.g., door lock/unlock);
- Change of values (e.g., zone occupancy count); and
- Access alarm events (e.g., lost access credential detected, door forced open condition).

Depending on the size of the access control system, thousands of events may be reported per day.

Modeling Access Control in BACnet

The extension of the BACnet standard for physical access control is built upon the existing BACnet model of objects and services, and uses existing objects and services wherever practical, with additional new objects to provide the required functionality. In BACnet, each object type represents a functional block or process within the application domain. The functional representation of an access control system in BACnet is an abstraction and does not depend on nor necessarily correspond to a specific hardware configuration or network topology.

A number of challenges needed to be addressed to adequately incorporate access control into BACnet, due to the unique operational characteristics and requirements of access control

systems. For example, access control involves a large number of transaction-based events, a situation not usually encountered in HVAC control. Access control requires a large and sophisticated database of users, credentials, rights and privileges, with a high frequency of changes. Many of the required objects are global, and, therefore, not constrained or even associated with a single device. The access control environment is both dynamic and mobile, with credentials being presented at different locations and times, creating a need to manage complex relationships between objects. Access control systems are also rapidly evolving, particularly regarding authentication mechanisms.

To facilitate this extension of BACnet, the access control system was decomposed into a set of related processes and interfaces. The concept of role-based access control (RBAC) was embraced for assigning rights and privileges for door access. This resulted in the development of seven new BACnet object types, in addition to the 24 existing objects, but no new BACnet services. One new event algorithm was developed, and other existing objects such as calendar and schedule were reused. The complete concepts and details are described in the white paper, "Physical Access Control in BACnet," which is available at www.bacnet.org/Bibliography/BAC-10-06.pdf. The following description presents a brief overview of the new BACnet objects for access control.

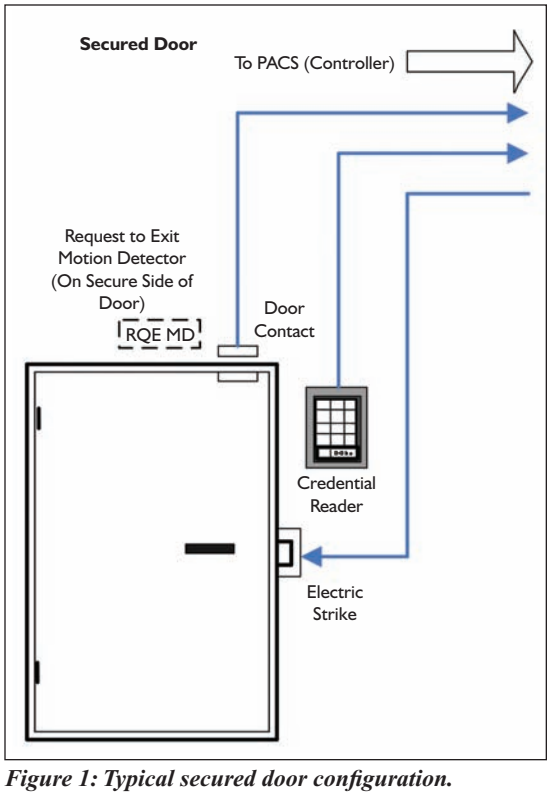

Figure 1: Typical secured door configuration.

Functional Decomposition, Interfaces and Objects

A PACS, as defined above, can be decomposed into a number of functional processes, which define visible interfaces. The interfaces are represented by a set of BACnet objects, which are standardized to enable interoperability among different implementations and vendors (see *Figure 2*).

The credential reader process reads authentication factors from access credentials. It performs validity checks such as parity bit verification, and provides the preprocessed authentication factor at its credential reader interface.

The authentication and authorization process receives authentication factors from the credential reader process at the credential reader interface, and performs authentication and authorization. The information used for this determination is exposed at the authentication and authorization interface. This process uses the access door interface to control the access door when access is granted.

The mechanical door control and monitoring process controls the physical door hardware. This hardware is abstracted into a uniform representation of an access controlled door and exposed at the access door interface.

BACnet PACS Object Model

The details of the BACnet PACS object model are shown in *Figure 3*. For each interface to the processes defined earlier, the BACnet objects comprising that interface are shown. Using standard BACnet methodology, an external system uses the interface by reading from or writing to properties of those objects.

The diagram also shows the relationship between objects within the model. An arrow pointing from one object to another indicates that the first object references or uses information from the second object while the accompanying text describes how the reference is used.

Credential Reader Interface

In most traditional PACS, the credential reader is wired directly to the controller through a local communication link such as Wiegand™ or EIA-485. In such cases, reading and processing the authentication factor is a local matter and typically is not exposed through BACnet. However, the access control extensions to the BACnet model allow for the authentication factor value to be network visible. This allows for nontraditional topologies where the credential reader and the controller are not directly connected but perhaps reside on a LAN, IP network, Internet, etc.

Authentication Factor Input objects represent the authentication factors read during a card swipe at the credential reader. Devices or objects that use this value can either poll intermittently or subscribe for change-of-value notification to determine when a new value has been read.

Some of the standard authentication formats to be added to BACnet are:

- Simple unsigned number from 0 to (almost) any size;
- Simple alphanumeric string;
- Structure of facility and card number (e.g., Wiegand-26 and proprietary Wiegand formats);

- FIPS 201 FASC-N number (agency code, system/site code, credential number);
- Standard biometric templates; and
- User name and password.

Authentication and Authorization Interface

The authentication and authorization process performs the traditional access control functionality as previously described. The BACnet objects that define the interface can be structured into elements for geographical organization (access point and access zone), and authentication and authorization (access credential, access user and access rights).

Access point objects represent the point where the authentication and authorization decision is made at a secured zone through an access-controlled door. Access through this point is directional in that it represents access in a single direction only. A door for which access is controlled in both directions (secured zones on both sides of the door) would be represented by two separate access point objects. The access point specifies the authentication policy that defines which authentication factors must be used to gain access to the secured zone at a specific time and is dynamically changeable. For example, access through the main office doors may require only a card swipe during regular office hours but may require a card swipe and biometric verification after hours.

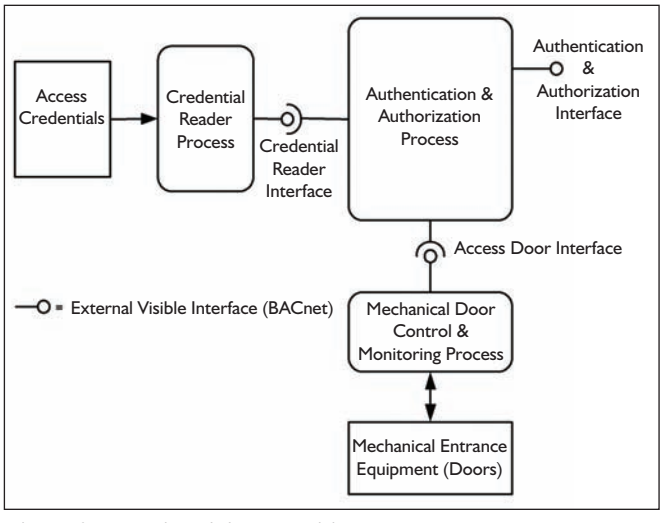

Figure 2: Functional decomposition.

The access point object generates events resulting from authentication and authorization. A new access event algorithm is defined, which allows the reporting of a broad set of events and transactions, along with fine grained filtering and prioritization capabilities. Event logging is achieved in a standardized way by using the event log object, which is in public review as part of Addendum *b* to Standard 135-2004.

The access zone object represents a secured zone that is defined by a geographically bounded collection of ingress and egress access points. The primary functions of the access zone enable occupancy counting, occupancy thresholds, passback detection and credential tracking. This object is optional and some simple access control systems will not support it.

The access credential object represents a container of related authentication factors such as card, PIN, biometric, etc. Authentication factors are grouped in a single credential when each factor has the identical access rights or when multi-factor authentication is supported (e.g., card and biometric). The authentication factors of an access credential may physically exist on the same media, such as a smart card (such as the FIPS-201 card), or may exist as physically separate entities, such as a card and PIN. Access rights objects are assigned to an access credential object to specify the rights of the access credential. Each access credential object may be assigned to a single access user. The state of the access credential determines whether the corresponding authentication factors are valid or invalid. An access credential may be invalid for a number of reasons such as if the credentials have expired, if they are not yet active, if they have exceeded the preset number of uses, if they have been manually disabled by an operator, etc.

The access user object represents a single person, an organizational entity or an asset. Relationships among access users are supported to model hierarchical organizations such as companies, departments, or groups of any kind, or to model ownership of assets. The access user object is not directly involved in the authentication and authorization process. It is used for informational purposes and may hold references or links to other systems. PACS implementations are not generally required to support this object type, although for some applications it may become useful. The access user object also lists which access credential objects are assigned to it.

Authorization is modeled with the access rights object. Each access rights object represents a common set of permissions or rights that are typically assigned together. For example, access permission to all perimeter doors (which may represent multiple access point objects) to a facility may be grouped together into one single access rights object. The structure of the access rights objects enables the hierarchical grouping of access rights that define a role. In role-based access control specific access rights (which may represent multiple access rights objects) are grouped together for specific groups of users. For example, the manager's role may allow unlimited access to the perimeter doors, all common areas and all conference rooms. Each manager in the facility would then inherit all the access rights of the manager's role as well as access rights to their own department.

A single access right consists of three elements.

1. The time when the access right is valid. This is typically the present value of a schedule object, but it may also be a computed value that represents some other external condition.

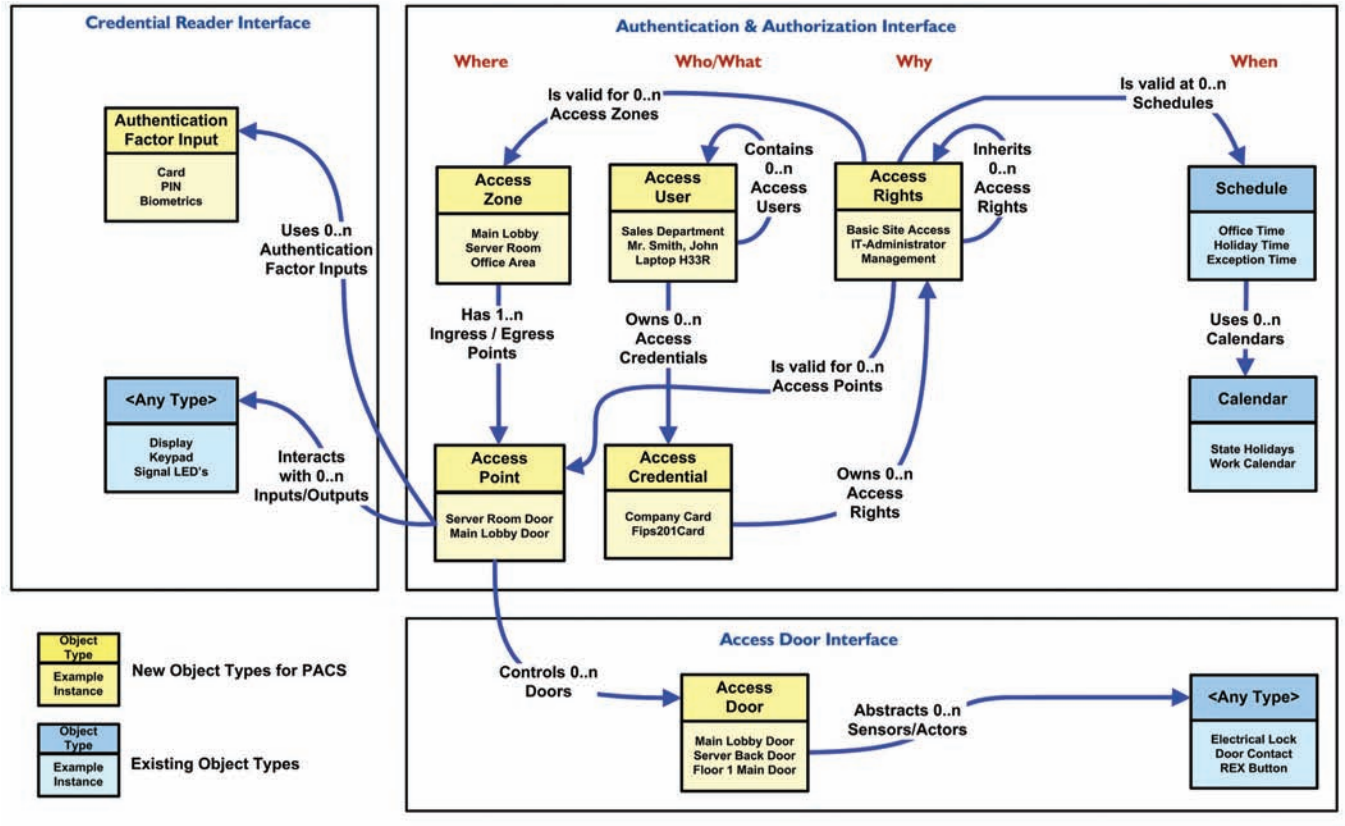

Figure 3: Overview of BACnet physical access control systems (PACS) model.

2. The geographical location where the access rights apply. This is either a specific access point or an access zone.
3. Optionally, the maximum threat level for which it is valid.

For the authorization process to succeed all three conditions of an access right must be valid, although there may be further conditions (e.g., passback violation, zone occupancy limitation, etc.) that cause the authorization to fail.

Access Door Interface

The access door object represents the combined and abstracted physical characteristics of an access-controlled door. This object has a relationship to all the physical door hardware and devices that are commonly associated with a door such as a door contact, door lock, request-to-exit, card reader, etc. Standard BACnet objects may be used to represent these individual components. For example, the door lock may be represented by a binary output, a supervised door contact by a multistate input, a request-to-exit button by a binary input, etc.

The access door typically is controlled by the authentication and authorization process, but may also be controlled by any of the other building automation system processes. The object arbitrates commands to lock, unlock or temporarily unlock the door through the use of the standard command prioritization scheme of BACnet.

The access door object also is responsible for generating alarms and events that correspond to the physical door using the standard BACnet change of state algorithm. Examples of access door-generated alarms and events are door-open-too-long, forced-open, tamper-alarm, etc.

The access door object is out for public review as Addendum *f* to Standard 135-2004.

Summary

The enhancements to BACnet to incorporate access control systems are intended to provide a robust and comprehensive capability that will be flexible enough to accommodate the range of existing and emerging systems. The model is scalable from the simple to large-scale enterprise-wide systems. While its original focus is on physical access control, it was developed to facilitate convergence of physical with logical access control, allowing one-card solutions. Since BACnet is a continuously evolving standard, participation of stakeholders, including manufacturers, vendors, systems designers and end-users, is always appreciated. Please refer to the BACnet Web site (www.bacnet.org) for relevant documents and contact information.