

Access Control for

Dealers
Users
Managers
Installers
Engineers
Salespeople

Presented by
SECURITY SALES®
& INTEGRATION

Part 1 of 4

Brought to You by



www.securitysales.com • MARCH 2008 A1

Access Control for

D.U.M.I.E.S. Part 1 of 4

Designer Access Control



Devising an electronic access control system begins with a detailed understanding of an end user's expectations and requirements. A system design can then be developed by following an initiative that aims to achieve four specific access control goals.

BY STEVEN O. GIBBS

Welcome to the latest of *Security Sales & Integration's* acclaimed "D.U.M.I.E.S." series: "Access Control for D.U.M.I.E.S." Brought to you by Pelco, this four-part series has been designed to educate readers about electronic access control system (EACS) design and implementation. "D.U.M.I.E.S." stands for dealers, users, managers, installers, engineers and salespeople.

This first installment in the series will cover the goals of system design, the process of preparing an accurate site survey, considerations for system communications and some discussion of final design end-product documents.

ACCESS CONTROL GOALS

The process of designing an EACS to meet the performance expectations of the owner/end user involves mixing appropriate technology with facilities management. Prior to beginning the development of an access control strategy, the system designer must understand what the user expects the EACS to accomplish by reviewing the four access control goals:

- Limit access
- Increase security
- Identify personnel
- Provide an audit trail

Each EACS is a balance of these four objectives. The success of the final system implementation is directly dependant on correctly identifying the needs of the user in each of these areas.

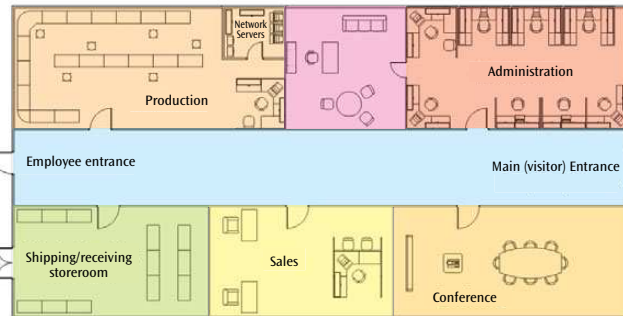
The first objective of the design process is to identify areas for which entry is to be controlled (i.e., access limited) by the EACS. The “Small Facility Floor Plan” diagram (right) depicts the layout and operations within a modest-sized facility. Before the introduction of electronic entry control, the first supervisor to arrive for work would use a key to unlock the employee entrance, which would be left open all day. Someone arriving from sales or administration would unlock the visitor entrance later in the day. Various departments would also have keys to enter their work areas when necessary. Obviously, the storeroom, production area and administration all have higher access limitations than the sales department or conference room.

‘PHYSICAL’ AND ‘VIRTUAL’ EXPLAINED

The designer needs to develop a system that controls access in two ways: physical and virtual. Physical restrictions are based on installing doors with locks and entry control devices to limit access. Virtual access restrictions are based on the programming of access levels and time zones.

The first opportunity for limiting access starts with the employee entrance. Once the door is unlocked, anyone (not just employees) can enter this door. Simply keeping this door locked all day and giving each employee a key is impractical. By placing an entry control device on the door, each employee can be given a code or credential that limits access to a specific door or doors — a physical limitation. A particular time period can instead be applied to manage access — a virtual limitation. If the credential holder is terminated or loses the credential, that single credential can be deleted from the system and there is no need to change locks and reissue keys.

Small Facility Floor Plan



Depicted is a layout and operations within a modest-sized facility. Electronic access control system (EACS) designers identify the various access points to determine the use of physical (e.g. doors with locks and entry control devices) or virtual (the programming of access levels and time zones) access restrictions.

The second opportunity for limiting access lends itself to the need for some personnel to have 24/7 access to the facility, such as senior administrators, security personnel and on-call maintenance workers. Without electronic entry control, the owner has no way of knowing when an employee has used his key to enter a facility. Almost every EACS creates a transaction with each access attempt that becomes part of the audit trail.

The third opportunity for limiting access comes from the need to allow some personnel limited access within the facility, while others may need additional or different access within the same facility. For example, production workers would not normally be allowed access into the network and server room, and administration and sales personnel would not generally be given access to the storeroom.

Virtual access restrictions are based on the programming of access levels and time zones in the EACS (see “Virtual Access Restrictions” on page A4), either at the local control panels in a small system or the software application program controlling a larger system. The restrictions include limiting access by day, time, door(s) and holidays.

The tools available to the system designer (and ultimately the system

administrator) to implement virtual access restrictions include: access levels, access codes, security levels, time codes and time zones.

These limitations are considered virtual because they can be changed in programming rather than by making physical changes to the system such as adding doors or locks. The ability to define access by groups of individuals rather than by each individual credential holder is very important for even the smallest of systems. The designer must also clearly determine the user’s needs for time codes.

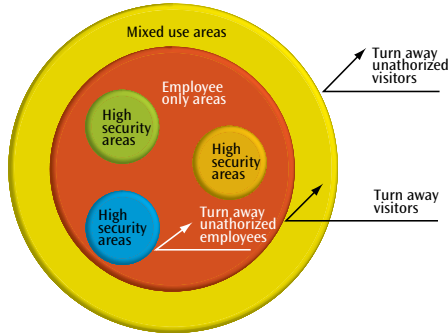
Keep in mind, even in a system with little need to control access by time of day or day of week, the system administrator may have a need to program many scheduled events. An example of this in the aforementioned small facility diagram would include unlocking and locking the visitor, administration office and sales department doors during normal business hours. However, the users in these three departments will likely desire a different unlock period for each door.

VARYING DEGREES OF RIGHT OF ENTRY

Although it would seem obvious no one would design and implement an EACS that did not increase security,

Access Control for D.U.M.I.E.S.

Rings of Control



The diagram represents the basic security concept of access control between the perimeter and the highest security levels inside a building. This illustrates the need for multiple access levels and a system that is flexible enough to expand as needed.

the degree of security the user wants to (or can) apply to the facility will also be a factor when choosing the type of controls placed on entry and exit points. Types and values of assets contained within an installation, and types and severity of any anticipated threat determine the security level required.

In many cases the system designer will rely heavily on risk assessment and vulnerability studies performed by the user. However, access controls at most federally-controlled facilities are now mandated by Homeland Security Presidential Directive (HSPD) 12 to meet the requirements and standards under Federal Information Processing Standards Publication (FIPS PUB) 201.

The system designer should identify the access points that are currently designated employee access only that have ineffective controls in place. In many cases, although policy and signs indicate these entry points are for employees only, many persons, such as visitors and other unauthorized personnel, are entering through these doors.

To what extent access will be limited within the facility will depend on how many different groups of employees exist within the facility, how many departments apply access control and how many areas of high-level security

will exist within the facility. Again, begin by looking for entry points with little or no controls in place that may be marked authorized personnel only.

Practically all facilities must accommodate visitors. The system designer must determine whether the user will wish to issue credentials to personnel who visit or work at the facility (such as outside contractors).

The continuum of parking controls extends from a small parking lot for employees located in a high-crime

area requiring tight physical security to a multiple lot facility for a large building with needs to reserve and separate parking for executives, employees, contractors and visitors. In many cases the designer will be specifying a system that must integrate with existing parking controls such as automated gates and barriers.

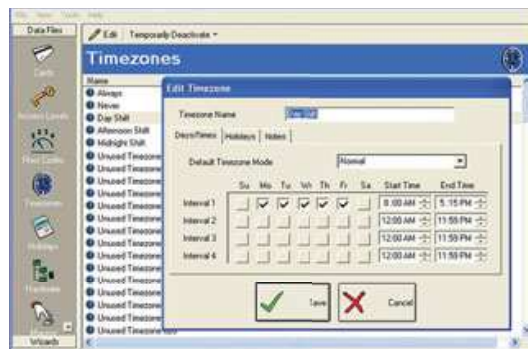
The "Rings of Control" diagram (left) represents the basic security concept of access control between the perimeter and the highest security levels inside a building. It can be modified and expanded to provide a conceptual representation of the user's needs by depicting the actual secured areas around and within the target facility. This will help explain the need for multiple access levels and a system that is flexible enough to expand with future needs.

CREDENTIALS IDENTIFY PERSONNEL

With any implementation of access control, identification occurs in two ways.

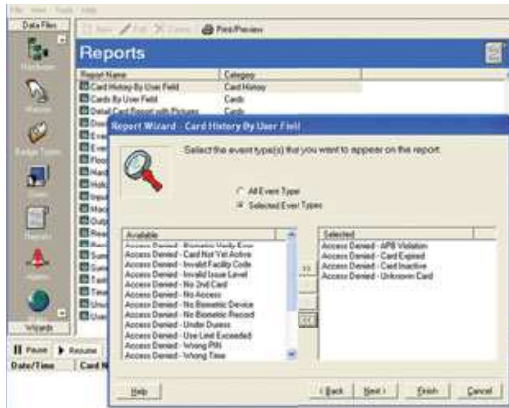
In the first method, the EACS identifies a specific number from a credential or keypad entry. Remember, the system is only identifying that a specific credential has access to the entry point, not that the person holding

Virtual Access Restrictions



The screenshot above illustrates virtual access restrictions based on the programming of access levels and time zones. Access levels and time zones are examples of virtual access limitations.

Audit Trail Report System



Audit trail or transaction reports are usually generated using report creation functions within the EACS software. This allows the user to select a transaction based on a combination of applied filters such as door name, credential holder, time frame and transaction type.

the credential is, in fact, the authorized user.

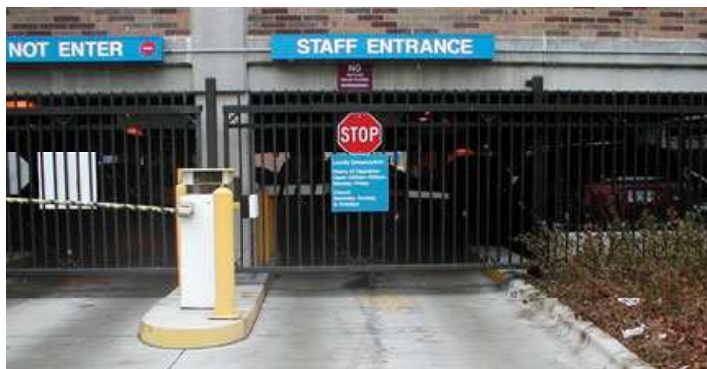
If additional verification of this person is needed then most credential-based entry control devices can incorporate a keypad into which a PIN must also be entered. Although this helps eliminate the casual use of a lost or stolen card it will not stop someone who intentionally lends another person their card and provides the PIN. When positive identification of an individual is needed, only a biometric entry control device can prevent someone from gaining access using another's credentials.

The second method of identification uses people to observe and identify each other by the use of an identification badge. This usually occurs on a casually or informal basis by personnel who, when noticing someone unfamiliar to them, check whether a person is wearing a proper identification card and whether it makes sense for that person to be in the facility or area.

Just about every implementation of an EACS using a card as the primary access control credential includes the integration of photo ID.

CREATING AN AUDIT TRAIL SCHEME

The system designer must carefully study the user's goals for an audit trail or transaction reporting system since not every EACS provides full functionality in this area (see "Audit Trail Report System"; left). The ability for an EACS to provide records of access attempts varies from a simple reporting printer that prints each transaction as it occurs up to a separate database engine such as Oracle® or Microsoft® SQL that can gen-



This electronic access control system (EACS) entry point is an example of a physical access control limitation. If a credential holder is terminated or loses the credential, it can be deleted from the system.

erate "canned" and "ad-hoc" reports on log files that might contain millions of transactions each year.

Small systems that may only have a printer attached will normally be able to print transactions as they occur. This is known as transaction logging. Transaction logging can also be utilized on larger systems that also store transactions for later reporting. In this case, important events such as alarms or access by certain individuals may be logged while more routine transactions are stored for later review.

When more than just a few doors and authorized personnel are involved in a system, a transaction log quickly becomes cumbersome and a waste of paper. Systems that utilize a computer for programming will also have the ability to store transactions on a hard drive for later review with a reporting tool. This is known as transaction reporting.

The next three installments of this "D.U.M.I.E.S." series will define and describe the many technical aspects of EACS design. However, many decisions the system designer will make about entry control devices, computer hardware and software, entry and exit point controls, alarm monitoring, and auxiliary control interfacing, will be based on the initial understanding of the user's needs in relation to the four access control goals.

Access Control for

D.U.M.I.E.S.



During the site survey process, door hardware details must be noted in order to properly specify electronic door control hardware. The device on the left is a rim-style latch; right, a mortise style.

SITE SURVEY UNEARTHS USER GOALS

Although the process of understanding the user's access control goals begins with face-to-face discussions, during the site survey process the system designer really begins to understand and document the user's goals. A complete and thorough site survey lays the foundation for implementing a system to meet the user's needs.

This site survey may take only a few hours (in the case of a small facility with few access points) to many weeks as would be the case with a major, statewide utility company with dozens of remote buildings. In most cases, several persons from the systems integrator's firm will be involved in the design process ranging from sales representatives, project managers and manufacturer representatives. The user may also need to involve several persons from their organization for input on design and project approval.

Since it would be impractical to have all these people participate in the site survey, the person performing the survey must collect and document the information about the site conditions that others will need to complete their overall system design responsibility.

Each entry control point should be given an appropriate and unique physical name that will later be used to populate the EACS software data-

base. Later in the design process a logical address will be assigned as the configuration of the system control panels takes place. For each named point a basic device listing will describe what hardware, such as readers, locking hardware and door monitoring devices, will later need to be specified. Enough information about the opening must be provided in order to properly specify the equipment.

This information must be followed by an operational narrative describing the groups or types of persons who will have access to this entry point, and whether this point will be continuously secured or unlocked by the system during specific times.

The information contained in the operational narrative will help the system designer determine how many access levels and time codes the EACS software and control panels will need to support.

Entry control points are not the only items documented during this process. For example, doors not controlled by the EACS should have a door contact switch connected to a monitor input point. Motion sensors may also be utilized to detect intrusion during specific periods of time. Again, each one of these should be assigned a unique physical name followed by a short device listing, plus an operational narrative.

Some entry points such as doors or gates may not be equipped with a credential reader. Rather, an auxiliary control relay from one of the EACS control panels will allow a door to be unlocked or a gate to be opened manually by a system operator or automatically during specific periods by a time code programmed in the EACS software. As with entry control and monitor points, each auxiliary control point should be described in the site survey document with a unique physical name, a device listing describing locking or control hardware, and an operational narrative (see "Door Hardware Details" on page A6).

Visit www.securitysales.com ("D.U.M.I.E.S." series section in the Special Reports link) to download a simple site survey describing the facility depicted in the "Small Facility Floor Plan" diagram and reviewed in the above access control goals.

EACS COMMUNICATION PARAMETERS

Unless the EACS will consist of only a few standalone entry control devices, it will be necessary for the EACS components to communicate with each other and the host programming and control platform.

Only a few short years ago, systems integrators had one choice when implementing an EACS: design: install and maintain a standalone, task-specific network of connected EACS devices.

This control panel network (CPN) would operate under one or more communication protocols such as RS232, RS422, RS485 and 20mA current loop. These protocols would be operated over cabling installed by the systems integrator and/or over dial-up or leased lines. The primary reason these networks were standalone was that most of the EACS devices utilized manufacturer-specific proprietary protocols. Although the physical layer (wire and electrical signal) used a standard such as RS232, the formats used for data transmission (language spo-

ken) were essentially different from system to system.

In recent years, with the proliferation of enterprise networks, systems integrators now have another option. Most organizations have some type of enterprise network consisting of a local area network (LAN) to provide communications for multiple platforms within their facilities. When connected to wide area networks (WANs), multiple buildings are connected together, whether they are across the street or around the world. These networks use TCP/IP to allow diverse systems and devices from thousands of different manufacturers to utilize the enterprise network as a communication backbone.

EACS manufacturers have responded with products from add-on cards for existing panels to panels with TCP/IP technology directly incorporated on the board in order to take full advantage of the current wave of IP convergence.

In the upcoming discussion of EACS hardware devices in Part II of this series, and communication networks in Part IV, the more technical aspects of this issue will be explained. However, during the site survey and system design phase the systems integrator must determine the existence of the network, whether it can be utilized, and locate access points (usually ports on the hubs and/or switches) to the network. Since network equipment closets and rooms are generally the connection point for EACS devices to the network and should have EACS controlled access, these are logical locations for placement of EACS intelligent control panels.

The system designer will need to work with the department within the user's organization responsible for the enterprise network during the early stages of design in order to obtain permission and coordinate access to the network.

DESIGN DOCUMENT TAKES SHAPE

The initial site survey and design process produces notes, drawings and



Since electronic access control system (EACS) control panels will most likely interface with the enterprise network, locating them in network equipment rooms throughout the facility makes sense.

data that will be used to create a system design document. What form this document takes is dependant on what stage the project has reached and the intended purpose of the document.

Several people within the systems integrator's organization will likely review the notes, survey documents and initial drawings to add information necessary to complete the system design. For instance, a particular manufacturer's product will be selected and model/part numbers will be specified for the various components identified in the site survey device listings. The person responsible for creating drawings will use notes, sketches and the drawings imported from the user's CAD files to create single line riser and device location drawings.

UNDERSTAND YOUR UNIQUE ROLE

"D.U.M.I.E.S." new to electronic access control systems, but familiar with video surveillance, intrusion or fire alarm systems, will surely recognize this system design process as being

similar to what they have used in the past. Hopefully, this basic design structure will allow each "player" to recognize their own role in this process.

Dealers are basically responsible for becoming familiar with the many solutions available to meet the security needs of the user. Users come to the table with the results of their own risk assessment and vulnerability studies, and are looking for assistance in implementing an EACS to meet their security goals. Managers or system administrators will normally be responsible for the initial data entry and programming of the EACS and maintaining the database of access levels, time codes and credential holders during day-to-day operations.

Installers will be called upon during the system design process to provide information concerning the installation of cabling, door control hardware and other EACS devices. Engineers may be associated with the system manufacturer and assist with product application questions or they may work for the systems integrator selecting appropriate system components. In today's IP convergence world, they will be the network engineers responsible for ensuring network bandwidth availability and coordinating the configuration of EACS devices for connection to the enterprise network.

Finally, salespeople are the ones responsible for coordinating the efforts of all other players, bringing them to the table at the appropriate times, and overseeing the process from initial contact with the user through system installation and commissioning.

The next three installments in this series will provide more detailed explanations of various aspects of EACS design and implementation relative to each of the above roles. ■

Steven Gibbs has more than 30 years' experience in access control systems performing installation, system design, project management and training functions. He can be contacted at (248) 373-8469 or steve@dvrtravel.com.