SAND--89-1113C

DE89 014781

DESIGN OF AN ADVANCED ENTRY CONTROL SYSTEM

J. Stephen Williams and David W. Miller

Sandia National Laboratories*

Albuquerque, New Mexico USA

ABSTRACT

An entry control system (ECS) allows the movement of authorized personnel and material through normal routes while detecting and delaying movement of unauthorized personnel and contraband. This paper presents an overview of several unique design and operating principles used in the implementation of a positive identity entry control system utilizing proximity cards. The system design incorporates distributed processing to support geographically separated entry points and redundancy such that no single point failure will shut down operations. The functionality and integration of the photo identification system, the visitor authorization system, and the access control and contraband detection system will be discussed. System unique features such as temporary badge issue for lost or forgotten badges at entry points using video lookup, visitor processing, and ergonomic and environmental considerations for the design of the proximity card based entry lane will be covered.

INTRODUCTION

The goal of an ECS is to allow the movement of authorized personnel and material through normal routes while detecting and delaying movement of unauthorized personnel and contraband. The system must be reliable and must be fast in its processing of personnel and presentation of information to the protective force.

To meet these goals, an ECS must

- o permit only authorized personnel to enter and exit the facility.
- o control entry at the perimeter where verification of authorized access is made. To further limit the access of authorized personnel, entry control can be extended into the facility to compartmentalize access.
- o detect and prevent the entry of contraband material such as weapons and explosives.
- o provide information concerning entry violations to the protective force.
- o provide a means to record and archive entry violations, operator actions, and other system events.
- o coordinate the operation of multiple portals and enrollment stations.

This paper presents the architecture and operating principles used in the implementation of a positive identity entry control system. The system is designed for installations with large populations requiring high throughput access at remote portals scattered over the facility. It complements the overall facility physical protection system to protect employees, classified and sensitive information, and property.

SYSTEM DESIGN

The system is based on a distributed processing architecture utilizing a centralized database with geographically-independent enrollment stations and portal locations. As shown in Figure 1, the ECS is divided into three major subsystems: the Access Control Subsystem (ACS), the Employee Enrollment Subsystem (EES), and the Visitor Processing Subsystem (VPS). The ACS contains the access control database and controls the entry of employees and visitors through the portals. The EES maintains the master employee database and enrolls employees into the ACS. The VPS maintains the master visitor database and enrolls visitors into the ACS. Each of these subsystems is discussed further in the following sections.

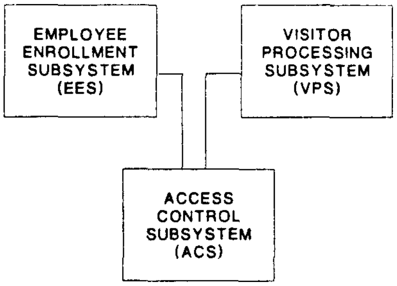
EMPLOYEE ENROLLMENT SUBSYSTEM (EES)
VISITOR PROCESSING SUBSYSTEM (VPS)
ACCESS CONTROL SUBSYSTEM (ACS)

Figure 1 Entry Control System Simplified Block Diagram

*This work was supported by the U.S. Department of Energy under Contract DE-AC04-76DP00789.

DISCLAIMER

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

DISCLAIMER

Portions of this document may be illegible in electronic image products. Images are produced from the best available original document.

Access Control Subsystem

The ACS is composed of two major components: a redundant host computer system and remote portal processors. The subsystem components are interconnected via a communications network, which can accommodate multiple transmission media (coax, twisted pair, and fiber optics). The ACS block diagram is shown in Figure 2.

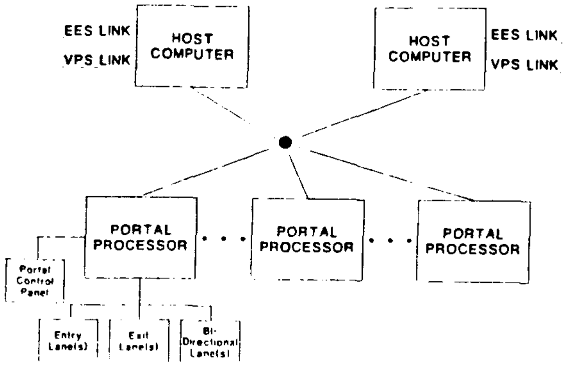

Figure 2 Access Control Subsystem Simplified Block Diagram

The host computer functions are:

- o Communications with the EES
- o Communications with the VPS
- o Maintenance of the master access control database
- o Download of data to the portal processors
- o Monitoring and coordination of the portal processors
- o System configuration
- o Access control report generation

The host computers are Intel 80386-based microcomputers.

A portal processor is located at each remote portal. The portal processor makes the decisions necessary to control access. Information about entry exceptions are presented to the protective force personnel stationed at the portal on the post control panel. The functions of the remote portal processor are:

- o Communications with the ACS host computers
- o Monitor and control of lane operations at the portal
- o Communication with lane control units
- o Present information to the protective force
- o Process input from the portal control panel

The remote portal processors are Intel 80286-based microcomputers.

The portal processor communicates with one or more lane control units which operate the following lane devices:

- o Badge reader device
- o PIN input device
- o Alphanumeric display
- o Badge capture reader
- o Flow control barrier (turnstile or gate)
- o Metal detector

Lanes can be configured as one-way or bi-directional and utilize three-arm or full-length turnstiles and strike-controlled swing gates. A lane reader station houses the alphanumeric display, the badge reader, and either the Personal Identification Number (PIN) input device in an entry lane or a badge capture reader in an exit lane. A reader station is physically attached to a three-arm turnstile; a pair of reader stations (one entry and one exit) is positioned on either side of a gate or full-length turnstile. The entry and exit reader stations are shown in Figure 3.

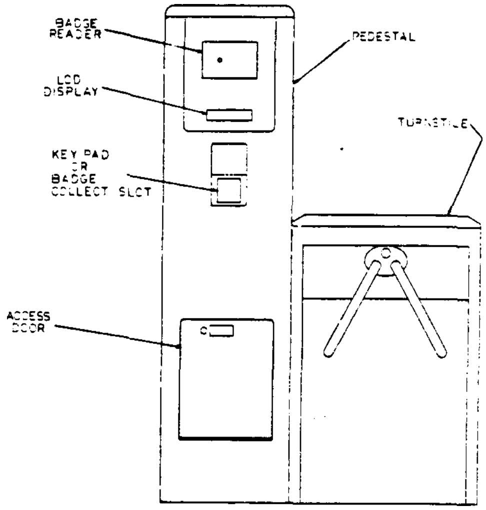

Figure 3 Entry and Exit Lane Reader Stations

The badge reader devices are proximity card readers based on operational ease-of-use criteria. A proximity badge is one in which the information can be read without placing the badge into the reader device. The badge draws its power from the reader unit as it enters the interrogation field and transmits its badge code to the reader. The PIN input device is a digital scrambler keypad which provides protection against PIN compromise. Walk-through metal detectors in the turnstile lanes and hand-held metal detector units at gate lanes are used to screen for weapons and contraband material. Each portal also has a conveyor belt X-ray machine to inspect packages and hand-carried items for weapons, explosives, or other contraband. Typical portal lane configurations are shown in Figure 4.

The portal processor also controls the portal control panel. This panel contains an alphanumeric display to present exception messages to the portal security personnel and lane override control push buttons for manual operation of the lanes by the portal security personnel.

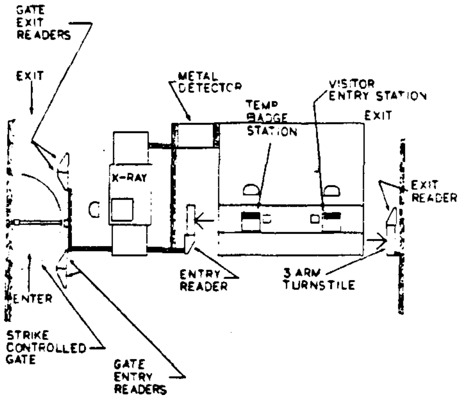

Figure 4 Portal Lane Configurations

Employee Enrollment Subsystem

The EES is a microcomputer-based local area network consisting of a file server, badge creation stations, enrollment workstations, temporary badge issue stations, and a communications processor. Figure 5 is a simplified block diagram for the EES. The EES maintains the biographic data, access information, and video image for employees on the file server. The access control information is passed from the EES to the ACS via the communications processor.

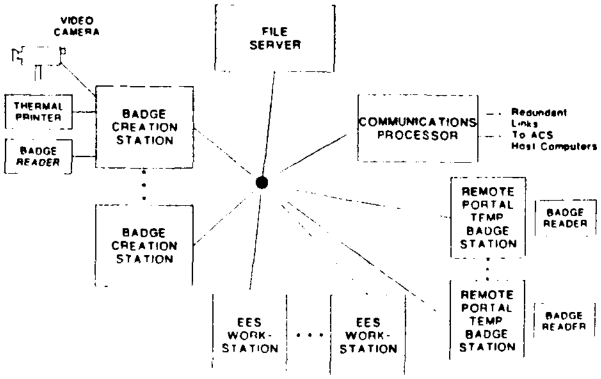

Figure 5 Employee Enrollment Subsystem Block Diagram

Badge creation stations are used to produce the photo identification badges. A video camera and thermal printer are attached to the station for this purpose. A proximity card reader and a hand-held numeric keypad are attached to the badge creation station to read the badge code and to enter the PIN.

Workstations attached to the network provide the capability to display the video image and to access the EES database to display and update text information. No video capture capability exists at these workstations.

Temporary badge stations are located at certain remote portals for the issuance of a temporary badge to an employee who has lost or forgotten his badge. A proximity card reader is attached to the temporary badge station for use in assigning a temporary proximity card badge to the individual.

Visitor Processing Subsystem

The VPS is responsible for scheduling approved visits and monitoring the entry of the visitors into the facility. The VPS is a fault-tolerant computer system with visitor control stations within the facility and visitor entry stations located at the portals. Figure 6 is a simplified block diagram for the VPS. The VPS communicates with the ACS to enroll authorized visitors so they can gain immediate temporary access to the facility. Information about visitor departures from the facility is passed from the ACS to the VPS automatically for historical recording.

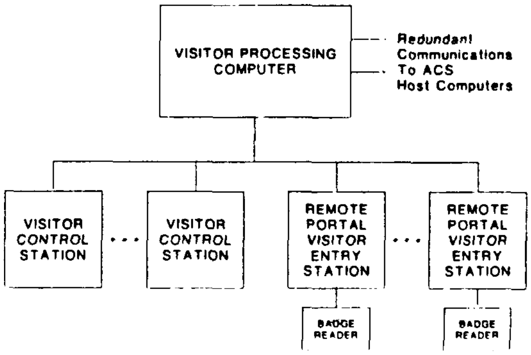

Figure 6 Visitor Processing Subsystem Block Diagram

OPERATIONS

Employee Enrollment

When an employee is enrolled in the EES, his biographic data, access privileges, video image, badge code, and PIN are recorded and stored in the master EES database. Certain fields of this database (name, badge code, PIN, and access privileges) are automatically forwarded to the ACS host computers to store in the master access control database. The badge code is entered by reading the badge with the reader attached to the badge creation station. A small hand-held keypad attached to the station is used by employees to select their PIN.

The photo identification badges are created by the EES on the badge creation stations. A video image of the employee is captured by a video camera attached to the badge creation station. The image is displayed on the station's video monitor; upon review of the image, the picture can be retaken immediately if necessary. When an acceptable image is captured, the station produces a high-quality badge insert containing the employee picture, name, and access level using a thermal printer. The insert is laminated immediately and affixed to the employee's assigned proximity card.

Visitor Processing

Visitors are entered into the VPS by authorized users at visitor control workstations when a visit has been authorized and the appropriate visitor clearances received and validated. Visitors are enrolled into the ACS by the VPS upon arrival at a remote portal visitor entry station. The visitor is processed by security personnel at the remote portal using the VPS to verify authorization for the visit. Once verified, the visitor is issued a proximity card badge. The badge is read by a reader attached to the visitor entry station and then the badge code and access information is forwarded to the ACS. The badge is activated at this time by the ACS and is only valid for a single entry.

Portal Operations

All portal activity is monitored by security personnel whenever the portal is accessible. They conduct package searches, respond to entry control exceptions and metal detector alerts, and issue temporary and visitor badges.

A portal has three types of lanes. An ingress lane consists of a proximity badge reader, a digital scrambler keypad, a turnstile, and a walk-through metal detector. An egress lane consists of a proximity badge reader, a badge capture reader, and a turnstile. The third type of lane serves as an ingress and egress lane for wheelchairs and personnel with handcarts or equipment. This lane consists of a gate, a proximity badge reader and digital scrambler keypad for entering, and a proximity badge reader and badge capture reader for exiting. A maximum of five lanes may be configured at a portal. A package x-ray scanner is located at the portal for use with the ingress lanes.

Employees and visitors place handcarried items on the conveyor belt of the x-ray scanning system before approaching a lane. Employees present the proximity badge to the badge reader and enter their PIN on the digital scrambler keypad. With verification of the PIN, the proximity badge activates the turnstile for one revolution. The visitor, having been issued a visitor proximity badge and enrolled in the ACS by the VPS, presents the proximity badge to the badge reader. Verification of an assigned badge activates the turnstile for a single revolution.

The individual (employee or visitor) then proceeds through a walk-through metal detector where he is scanned for metal. If the person is not a facility security officer or otherwise authorized to carry a weapon and appropriate quantities of metal are detected, an alarm is sounded locally and portal security personnel approach the person and assess the alarm. If portal security personnel are satisfied there is not a threat associated with the alarm, the individual is permitted access to the facility. Visitors then retrieve the handcarried items from the x-ray scanner conveyor belt.

A gate entrance is for personnel using a wheelchair or cart. The individual approaches the gate and presents the proximity badge to the reader and, if not a visitor, enters his PIN on the digital scrambler keypad when prompted. If it is a valid entry, a local alarm is sounded to notify portal security personnel that someone is at the gate requesting access. Portal security personnel approach the gate and conduct the search for contraband. If the contraband check is negative, portal security personnel activate a switch which opens the gate allowing entry to the facility. Portal security personnel maintain visual observation of the gate to prevent tailgating.

Exception Processing

Visual and audio indications are generated at the portal to alert the portal security personnel to access control exceptions at any of the portal lanes. The portal control panel generates an alarm tone and displays a message indicating the exception and the lane at which it occurred. The alarm tone is silenced by the portal security personnel and the exception message is viewed. Portal security personnel review the exception and take appropriate action. Exceptions reported at the portal include:

o Invalid badge
o Zone violation
o Time violation
o Expired badge
o Maximum PIN attempts exceeded
o Lane equipment failures

Access will be denied to users who repeatedly fail to enter the correct PIN. This is done to preclude compromising the entry control system by systematic iteration of possible PIN combinations. If a user fails to enter a correct PIN, a PIN-attempts counter for the individual (maintained across all portals) is incremented. A successful PIN entry resets the counter to zero. If a user exceeds the maximum number of PIN attempts allowed, the portal security personnel are notified. All subsequent invalid PIN attempts by that user will alert the portal security personnel until a valid PIN is entered.

FEATURES

Temporary Badge Issue

Temporary badge stations are placed at strategically located remote portals for the issuance of a temporary badge to an employee who has lost or forgotten his badge. Portal security personnel use the temporary badge stations to access the EES database to retrieve the photo image of the employee and verify his access privileges. A temporary proximity card badge is issued to the employee and read by a proximity card reader attached to the temporary badge station. The permanent badge number for the employee is made inactive at this time until the individual returns the temporary proximity badge. The EES will notify the ACS via the communications processor to deactivate the permanent badge and activate the temporary badge. An employee who is issued a temporary badge will be prompted by the system to surrender the temporary badge to the badge capture reader when the individual exits the facility. When the temporary badge is surrendered, the individual's permanent badge is reactivated and the temporary badge deactivated by the ACS. Only one badge per individual is activated at any time.

Temporary and Visitor Badge Capture

When a visitor or temporary badge holder exits the facility, the proximity card badge is read by a reader at an egress lane. The badge holder is then prompted to insert the badge into the badge capture slot. When the badge capture reader determines that the badge has been returned, the turnstile is unlocked, and the badge holder exits the facility. The visitor badge or temporary badge is disabled at this time and is no longer valid for entry. Information about visitor departures is sent to the VPS by the ACS.

Anti-Passback

The system incorporates the anti-passback feature. A badge cannot be reused for multiple successive entries into an area. This prevents an individual from passing his badge to another individual for use.

Authorized Access Times

The system provides an authorized access times feature. An individual's access privilege can be limited to specific days of the week and hours of the day which comprise the work period. Entry to the facility on holidays can also be controlled.

Host Computer Redundancy

The use of dual host computers provides considerable redundancy. Each host computer is connected to the EES communications processor, the VPS computer, and the remote portal processor communications network. If the main computer fails, the backup computer automatically assumes control of the communication links and operations continue normally.

Standalone Portal Operations

The host computer system downloads access control information received from the EES and the VPS to each of the portal processors. A portal processor transmits its entry and exit activity to the host computer system, which in turn updates the other portal processors. If the communications fail due to loss of the host computer system or the network facilities, the portal processor operates in a standalone mode. Each portal processor maintains its own subset of the master ACS database so that loss of communications will not significantly affect local portal activity. The portal processor only allows access to individuals enrolled in its database prior to losing communication with the host computer system. The portal processor maintains a database of the entry and exit events that have occurred since the communications failure. When communications are restored, the information is sent to the host computer system to update its database and the other portal processors. Updates received by the host computer system from the EES during the communications failure are sent when communications with the portal processor is restored.

Manual Overrides and Fail-Safe Operation

The turnstiles and gates utilized in the system have a fail-safe capability which unlock the device and allow it to remain open in either direction during a power failure. Further, manual override capabilities are provided to the portal security personnel. The portal control panel contains override control push buttons which release each turnstile or gate for one passage, and an emergency override button which latches the turnstiles and gates in the unlocked bi-directional state for emergency evacuations.

System Response

The system is capable of processing a steady flow of personnel into the facility. No degradation in response was noticed at a fully configured portal with continual lane activity. Presentation of information to portal security personnel is instantaneous. Picture image recall at a temporary badge station is on the order of two-three seconds. Printing time for a badge photo insert in less than one minute.

SPECIAL CONSIDERATIONS

Ergonomic Design of Lane Reader Stations

An ergonomic study was conducted to determine the optimal placement of the components in the portal lane reader stations. The analyses was conducted for both walking and wheelchair users. Concerns addressed by the study were the display and keypad visibility and the badge reach ranges. The analyses were based on U.S. male and female population ranging from the 2.5 to the 97.5 percentile. Acceptable visibility and reach ranges were determined for each component, and optimal placements were arrived at by taking additional criteria into account such as the minimum separation of components to prevent interference.

Component Environmental Testing

Environmental testing was conducted on portal lane equipment to ensure proper operations of outdoor lanes. Testing included a rain test of approximately one inch per hour and a multi-cycle temperature and moisture resistance test. The multi-cycle moisture resistance test consisted of a hot cycle of 93°F with 95% relative humidity followed by a cold cycle at -10°F. The components were tested in an operational configuration and included proximity cards, card readers, keypads, displays, badge capture readers, turnstiles, and metal detectors.

Badge Laminate Packets

An evaluation of various laminate packets was conducted to assess their suitability for use with the badges. A series of environmental and mechanical tests were performed to determine the durability of the laminate packet, thermal insert, and adhesive. A laminate packet with a thermal adhesive was determined to provide a long-lasting high-quality image of the thermal paper insert.

SUMMARY

Although entry control requirements are similar at many facilities, operational concerns and constraints have led to the implementation of several unique design features for the ECS presented in this paper. These concepts utilize commercially available off-the-shelf state-of-the-art access control and video imaging hardware and software packages to provide a fast, reliable, and user-friendly system. The system achieves high personnel throughput, minimizes operational impacts, and complements the facility physical protection system.