4/18/2013

ADVANCED IMAGING SYSTEMS

10617 SOUTHERN LOOP BLVD
PINEVILLE, NC 28134
PHONE (704) 525-4392
FAX (704) 252-4393
www.aisimc.com

167986

7

CONF-820713--3

SAND82-1229C

AN ENTRY CONTROL SYSTEM FOR LARGE POPULATIONS

MASTER

Paul D. Merillat
Sandia National Laboratories
Albuquerque, New Mexico 87185

SAND--82-1229C

DE82 017033

ABSTRACT

An Entry Control System has been developed which is appropriate for use at an installation with a large population requiring access over a large area. This is accomplished by centralizing the data base management and enrollment functions and decentralizing the guard-assisted, positive personnel identification and access functions. Current information pertaining to all enrollees is maintained through user-friendly enrollment stations. These stations may be used to enroll individuals, alter their area access authorizations, change expiration dates, and other similar functions. An audit trail of data base alterations is provided to the System Manager. Decentralized systems exist at each area to which access is controlled. The central system provides these systems with the necessary entry control information to allow them to operate microprocessor-driven entry control devices. The system is comprised of commercially available entry control components and is structured such that it will be able to incorporate improved devices as technology progresses. Currently, access is granted to individuals who possess a valid credential, have current access authorization, can supply a memorized personal identification number, and whose physical hand dimensions match their profile obtained during enrollment. The entry control devices report misuses as security violations to a Guard Alarm Display and Assessment System.

DISCLAIMER

This book 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.

NOTICE
PORTIONS OF THIS REPORT ARE ILLEGIBLE.
It has been reproduced from the best available copy to permit the broadest possible availability.

INTRODUCTION

Controlling access to general and critical areas of a nuclear facility is a common technique used to help prevent

DISTRIBUTION OF THIS DOCUMENT IS UNLIMITED

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.

acts of sabotage and theft. Managing access control becomes more difficult as the number of authorized people increases and as the size of the area under control grows. Sandia National Laboratories has developed an entry control system appropriate for use at an installation with several thousand people requiring access over an area encompassing many square miles.

- The system is capable of supporting automated personnel identification devices. Several types of devices offering an improvement over guard-examined picture-badge systems are available or are being developed by the commercial sector. This system uses an identification device which compares a subject's hand dimensions against those obtained during enrollment. The system approach is general enough to allow the incorporation of new or improved identifiers as they become available.

REQUIREMENTS

The general requirements of the system are not unique to a specific installation. The goals of this particular system are as follows:

1) A population of up to 10,000 people may be simultaneously enrolled;

2) These users require access to remote sites which are separated by distances of several miles;

3) The remote sites are divided into distinct areas in such a manner that an individual user may have access to some areas and not to others;

4) Because of safety requirements, current occupancy lists of areas and sites may be generated locally or from a central control point;

5) No single point failure will prevent the system from operating and multi-point failures will have limited effect;

6) The system will interface with an automated security system by reporting unauthorized user movement across a protected boundary;

7) The data base must be easily managed and changes to the data base may be followed by an audit trail.

The system design was significantly influenced by the size of the user population and the large area over which the population could have access. The general approach was to centralize the data base management and enrollment functions and to decentralize the guard-assisted entry control functions.

THE DATA BASE MANAGER

The data base is maintained at a central site, ideally at the badge office in an administration building. The Data Base Manager, a Digital Equipment Corporation LSI 11/23 microcomputer, is responsible for maintaining the integrity of the data base. This is a hard disk-based system on which the user information is stored. The Data Base Manager supports up to four enrollment stations through which modifications to the data base are made. These enrollment stations may be collocated with the Data Base Manager or may be configured as satellite stations many miles distant. No access control functions are performed by this part of the system.

The Data Base Manager is controlled through a System Manager's terminal. The System Manager is the individual responsible for the operation of the entry control system. Through his private terminal, he may obtain reports which allow him to manage the system. These reports include audit trails of the changes to the data base, system status reports, and various types of data base listings. It is through this terminal that occupancy lists of any of the remote areas or sites may be initiated.

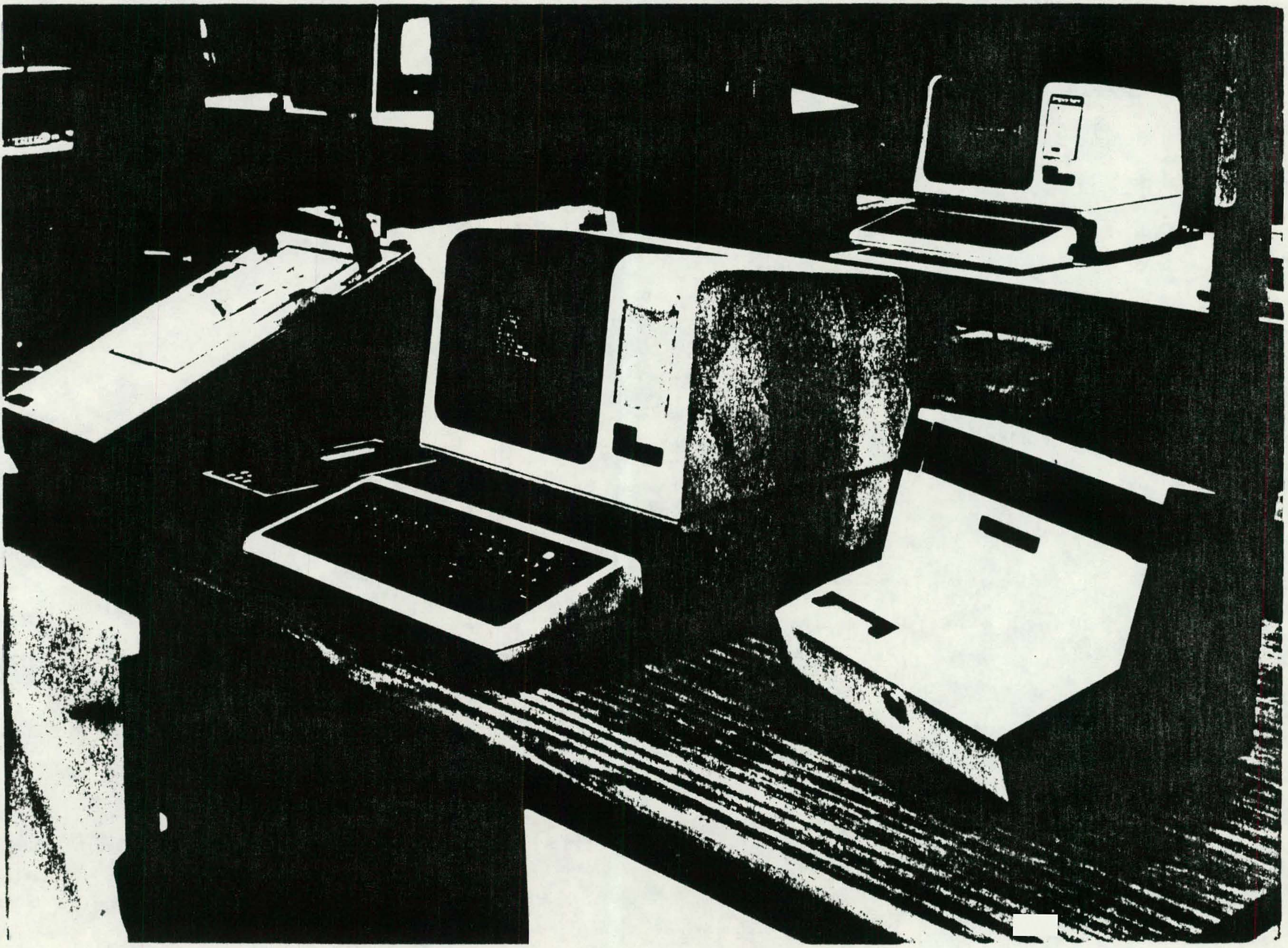
The user's first contact with the system is through an enrollment station operator. In order for the user to gain access to a protected area, he must be issued a badge with an encoded magnetic stripe. This badge references the user's file which contains a personal identification number (PIN) and his hand geometry. It is at an enrollment station that the user's hand geometries are measured and a PIN issued. Figure 1 shows a typical enrollment station configuration.

The password-protected enrollment stations are activated through the System Manager's terminal. The enrollment stations may be deactivated by an enrollment station operator or by the System Manager. An enrollment station consists of four devices. These are a video terminal, a Stellar Systems ID2000T1 Identimat, an Entrec badge reader, and an Elcom Industries magnetic stripe badge encoder.

The enrollment station operator interacts with the Data Base Manager through the video terminal. Forms Management, a special software package supplied by Digital Equipment Corporation, is used to present a user-friendly interface to the enrollment station operator. The operator is presented with various activity menus and based on the selection will fill in various information fields. The operator may enroll users, examine user's file, encode badges, allow a user to practice identifications, issue temporary badges, cancel badges, and re-establish hand geometries.

The enrollment procedure is typically a two-step process. Administratively, it will be decided that a new user is to have access to certain areas under the control of the system. An enrollment station operator can then pre-enroll this user by entering his name, employee number, access authorization, expiration date, and a few control codes. The badge may also be encoded at this time. Later, the new enrollee is called

FIGURE 1.



in. His hand-geometry measurements are taken and he is issued his badge and PIN. The operator will then show him how to use the system and allow him to practice before going out to the remote area.

THE REMOTE SITE SYSTEMS

Figure 2 shows the system configuration.

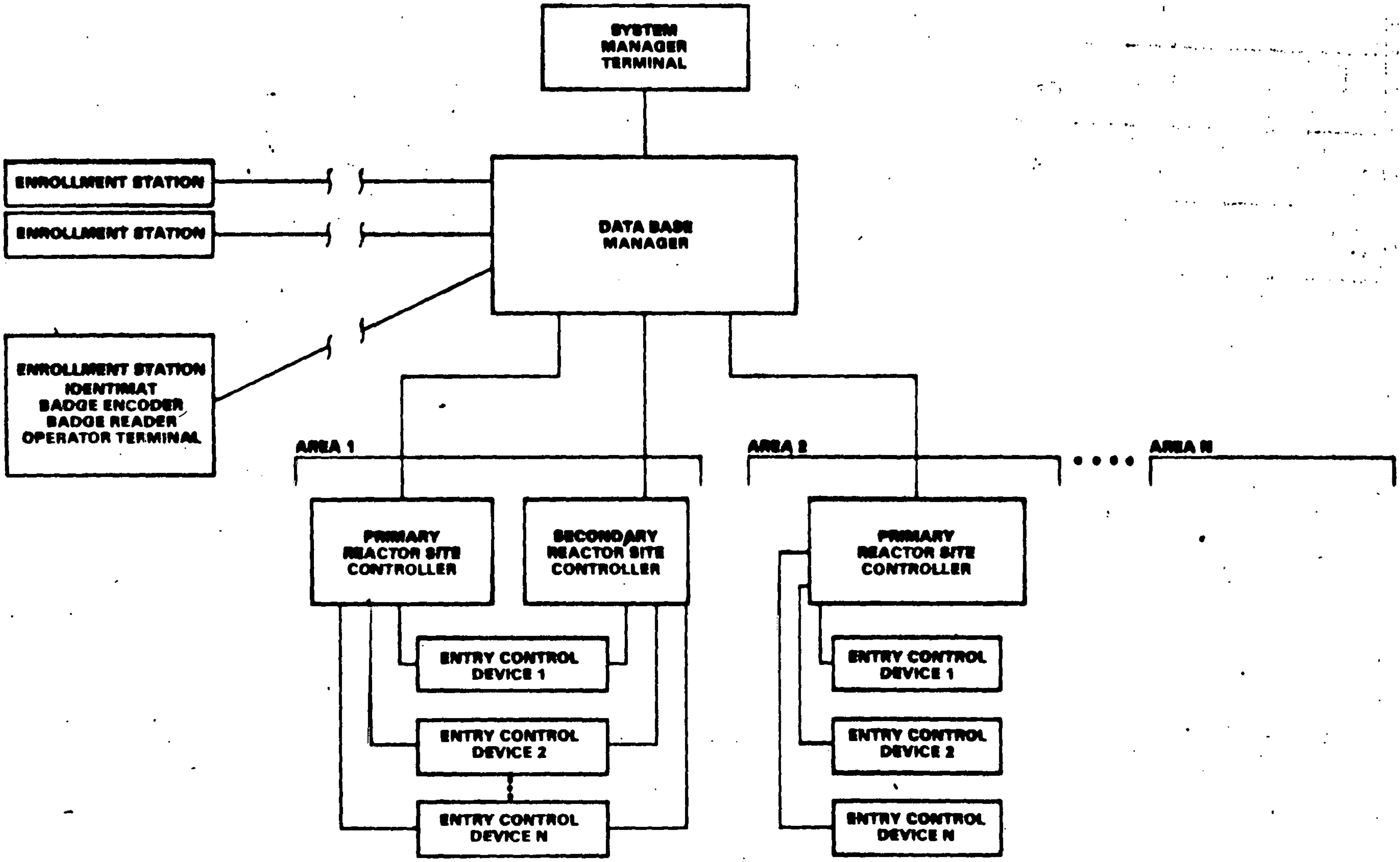
Each remote site has a pair of Remote Site controllers. These are Digital Equipment Corporation LSI 11/23 hard disk-based microcomputers. Each of these Remote Site controllers is connected to the Data Base Manager along dedicated telephone links. When the Data Base Manager receives a change to its data base which affects the entry control function, it will pass this information to all affected Remote Site controllers. In this manner, each Remote Site controller has enough information to perform the entry control function indpendent of the Data Base Manager.

There are two Remote Site controllers at each site in order to provide redundant operation of the entry control devices. If one of the Remote Site controllers has failed, no degredation of the entry control operation will be observed. If no need exists for the redundant operation, only one Remote Site controller is installed.

Each Remote Site controller is connected to all the entry control devices at the remote site. The entry control devices are microprocessor-based. A very simple communications protocol is used between the entry control devices and the Remote Site controllers. When the entry control device needs a file, it makes a file request to the Remote Site controller. The Remote Site controller will verify area authorization, check for can-

FIGURE 2.

ENTRY CONTROL SYSTEM CONFIGURATION

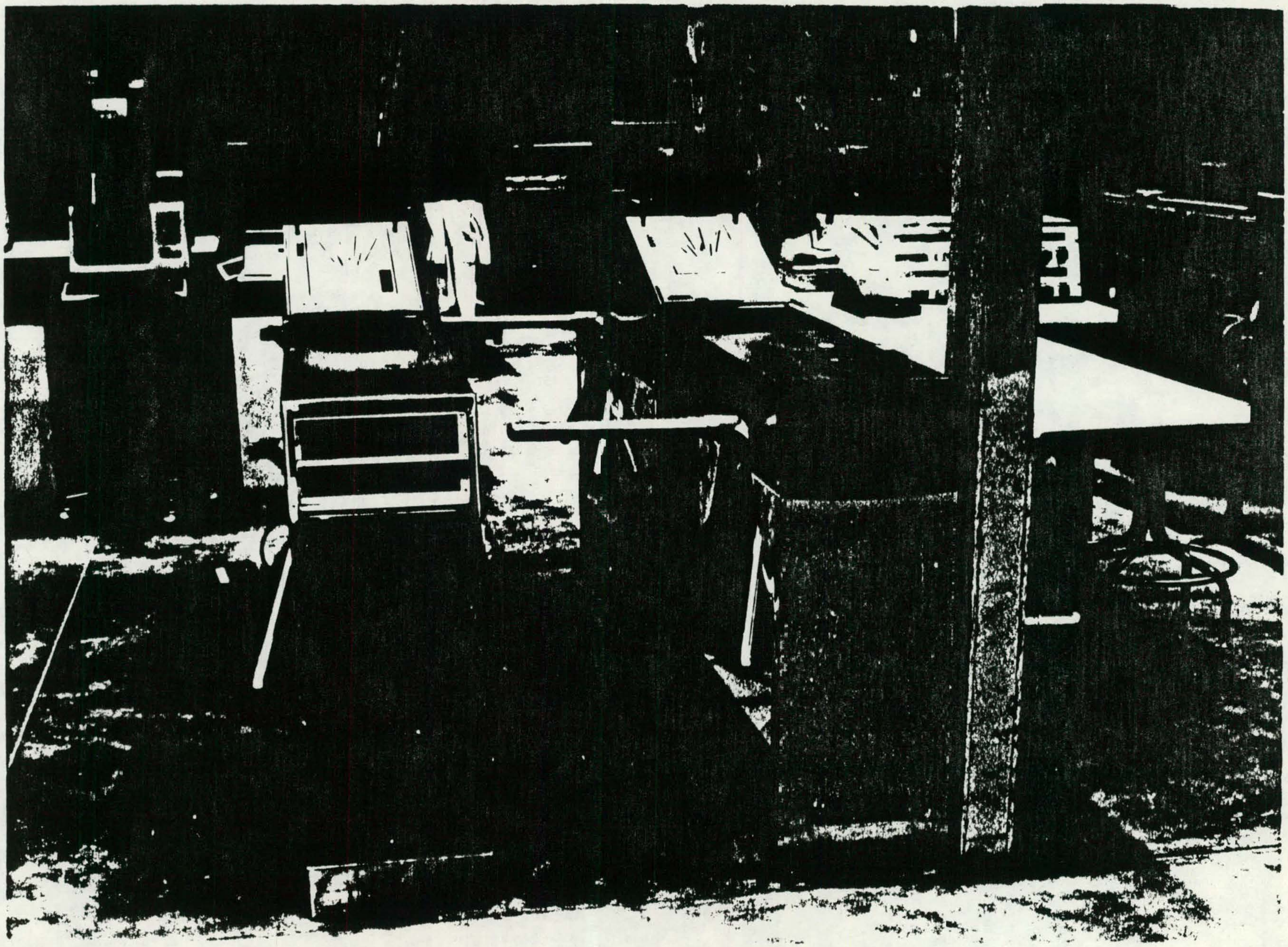


cellation and expirations, and if all is well, it will deliver the file to the entry control device. If the entry control device cannot get a response from one Remote Site controller, it will try the other. When the entry transaction is finished, the entry control device will send a status message to both Remote Site controllers. This message informs the Remote Site controller of the new position of the user as well as information pertaining to the passage.

The heart of the entry control devices in this system is the Stellar Systems Identimat. This device compares four finger lengths of a specified hand with that taken at enrollment. The user passes if his individual finger lengths agree with that stored in his file within a specified tolerance. The Identimat is a microprocessor-controlled device and contains an adaptive algorithm. If a user successfully uses the device, the adaptive algorithm allows for slight changes in the user's hand geometry. Over time, most users become more consistent with their use so their hand geometries stabilize and their tolerances decrease.

The entry control device for pedestrian traffic is a dual turnstile lane. Figure 3 shows this configuration. High traffic areas will have several lanes operating in parallel. A user wishing to gain access to a protected area will approach one of the lanes. He runs his badge through the badge reader and keys in his PIN. If he has access authorization and his PIN is correct, the outer turnstile will unlock and the user may proceed forward. An Identimat hand-geometry verification device is located in the lane between the two turnstiles. When the user reaches this point, he will place his hand on the Identimat to have his hand geometry verified. If the verification was successful, the inner turnstile unlocks and the user may proceed into the protected area. A user wishing to leave a protected area approaches one of the lanes. He runs his badge through the badge reader causing the inner turnstile to unlock.

FIGURE 3.



The user proceeds through the inner turnstile which causes the outer turnstile to unlock. The user then exits the protected area. PIN and hand-geometry checks are not required for egress.

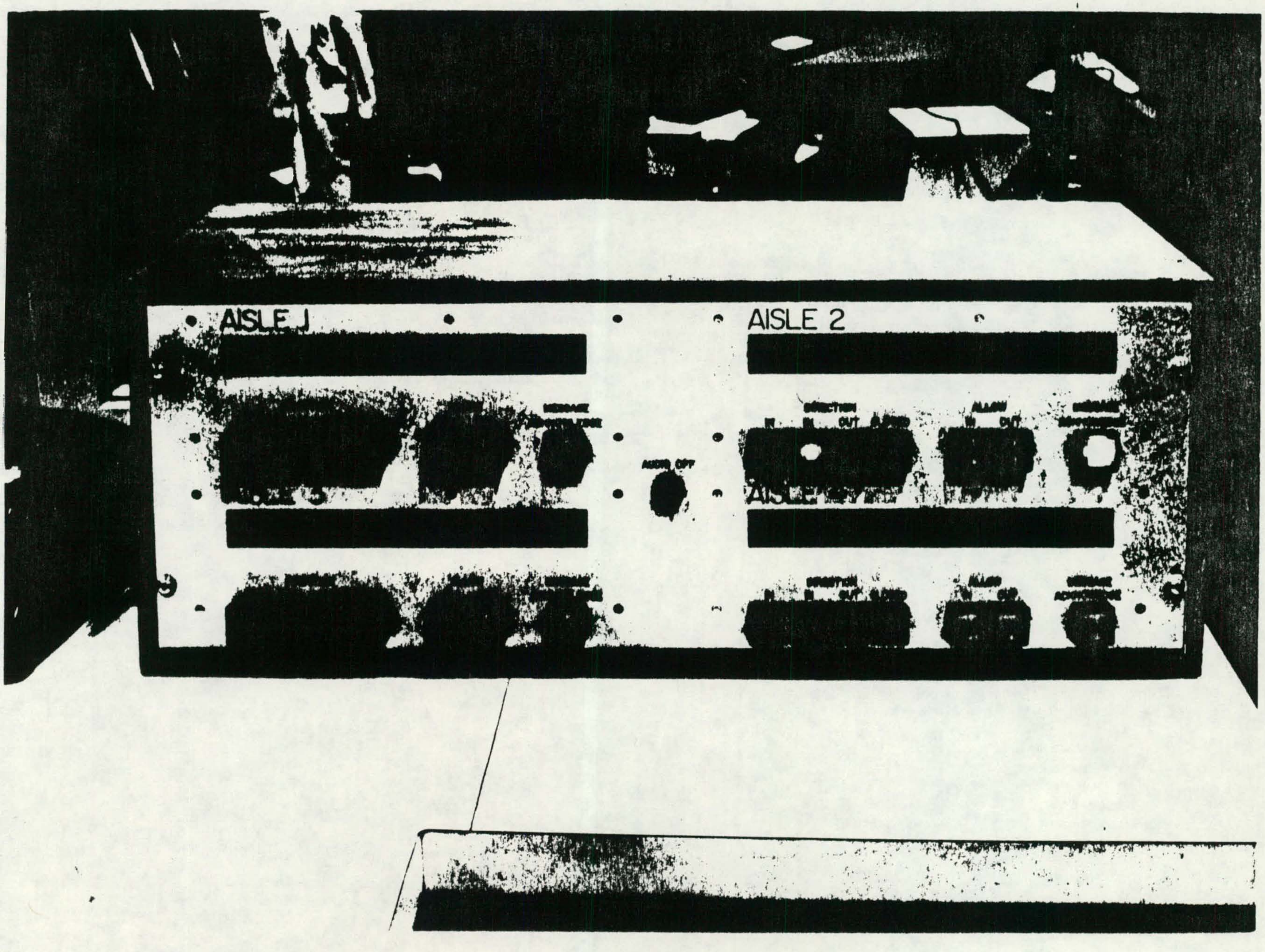
The entire procedure is performed in view of a guard. The guard visually monitors the activities of the lanes. He also has a Guard Display Unit with which each entry control device communicates. Figure 4 shows a four-lane Guard Display Unit. The guard uses the Guard Display Unit to configure the lanes. He may select lanes as "In Only", "Out Only", "Bi-directional", or "Off". Any problem arising from the use of the lanes is annotated on a character display. Messages which appear on the character display inform the guard of failed devices, cancelled and expired badges, failed hand geometries and PINs, and special circumstances such as no hand geometry required. The guard will have procedurally defined actions to take for each message. For the case of escorted visitors, the guard has the ability to override the entry control device and to allow a user in or out. In this case, the user must be manually logged into or out of the area by the guard.

The guard may also interact with either Remote Site controller to obtain an occupancy list. This is the same list which may be obtained by the System Manager at the System Manager's terminal.

Infrared sensors are installed at the inner turnstile to form a protected plane. When the entry control device unlocks the inner turnstile, it masks this sensor. If the protected plane is crossed without permission by the entry control device, an alarm is sent to the automated security system.

Vehicle occupants wishing entry into a protected area must leave their vehicle to use the pedestrian lanes. The guard will insure that all occupants have used the pedestrian lanes. The

FIGURE 4.


AISLE 1
AISLE 2
DIRECTION
IN
OUT
ALARM
IN
OUT
MESSAGE
AUDIO OFF

guard typically will also check for contraband in the vehicle. If all the occupants pass the entry control checks, they may then enter the area in their vehicle. Occupants of vehicles wishing to leave a protected area will have their badges collected by the guard. The guard will run their badges through a special vehicle exit reader to log the occupants out of the area.

There is nothing inherent in the system design which precludes other types of entry control devices from being used. The simple protocol used between the entry control devices and the Remote Site controllers allows simple door lock control devices or complex unattended booths to be part of the system. Furthermore, the entry control devices may interface to other systems such as radiation monitoring and control systems or personnel monitoring systems.

SPECIAL FEATURES

Special features are implemented in this system as a result of problems in maintaining entry requirements for large populations. The first is that temporary area authorization may be granted. Large installations often have people who require access into critical areas only rarely. This may be as a result of maintenance or inspection requirements. Through an enrollment station, temporary area access may be granted to an individual for a defined period of time. After that time is up, his authorization reverts back to his permanent area authorization.

A group code may be associated with each user. This enables the installation to set up work teams which require access to specific areas at the same time. A special group change function is available at the enrollment stations. All members of a group may be granted authorization into a specific area for a specific length of time by means of a single enrollment station operation.

Individuals may also be assigned predefined tags which further identify them. This could be used to mean a user is a member of a safety team or knows CPR. During emergencies, this information could be obtained as part of the occupancy list to enhance response to a problem.

INFORMATION FLOW

A Remote Site controller pair and the entry control devices within a remote site essentially form a stand-alone system. File requests and status messages are the only messages which are transmitted between these two types of devices. The Remote Site controllers are polled every three minutes by the Data Base Manager. At this point, the Remote Site controllers will report significant events which have occurred since the last poll. These events are that a specific user has updated his hand geometry, that a user's badge has been cancelled due to three consecutive failed entry attempts, or that the Remote Site controller has just been re-started and requires the current occupancy list from the other controller.

The Data Base Manager will propogate updated hand geometries and badge cancellation events to the other remote sites. Once a day, at midnight, the Data Base Manager will scan the data base looking for badges which have expired. Badge expiration messages are then sent out to the remote sites. Once a day, at 3:00 a.m., the Data Base Manager will request statistical usage information from each of the remote sites. Statistics are kept by user on the number of attempts and the number of failures.

When an occupancy list is requested through the System Manager's terminal, the Data Base Manager will obtain the occupancy information from the specified Remote Site controller pair. The Data Base Manager is also responsible for transferring an occupancy list from one Remote Site controller to a recovering Remote Site controller.

When a change is made at an enrollment station which affects the entry control function, the Data Base Manager will send an update to the affected remote sites.

If a Remote Site controller is down when the Data Base Manager tries to send an update, the message will be saved on disk for transmission when the Remote Site controller is re-started.

This approach ensures that the failure of any of the computers will not result in the loss of the entry control function. If the Data Base Manager is not operational, the Remote Site controllers will operate on the data which was current at the time of failure.

OPERATIONAL IMPACT

Most of the operational impact will occur early in the implementation of the system. Clearly, installation of such a system is a large task and should be done in phases. The enrollment of the existing population is also time-consuming. An enrollment can be completed in about five minutes although the average time may realistically approach ten minutes.

It will also take more time for a user to pass a protected point than with a guard-examined picture-badge scheme. Timing tests indicate that a single user requires about 15 seconds to use a dual turnstile lane for entry. Queues of users are handled on average more rapidly since one user may be reading his badge and entering his PIN while the previous user is using the Identimat. The average time for users in queue is about ten seconds. Time for exit is about four seconds.

Use of the Identimat itself will pose some problems. Most of these problems will occur during initial use. Some training is required to become consistent with the use of the device. There will be a small fraction of the population (typically less than 1%) who simply cannot use the device. People with arthritis or poorly-formed fingers often have trouble. The system caters for these people by allowing a user to be enrolled with his hand geometry waived. The guard must manually identify these users.

SUMMARY

This system is designed to be a part of a more comprehensive security system. The entry control functions are in balance with intrusion detection and assessment equipment, and guard-response mechanisms. The data base management and enrollment functions are centralized, while the positive personnel identification and access functions are decentralized. An adversary attempting to defeat the system requires possession of a valid credential, knowledge of the memorized PIN, area authorization, and a hand-geometry match.