CONF-8 [illegible]-1

[redacted]

[redacted]

Work Performed Under Contract DE-AC09-78ET-35900

ALLIED-GENERAL NUCLEAR SERVICES
P.O. BOX 847
BARNWELL, SC 29812

DISCLAIMER

Printed in the United States of America
Available from
National Technical Information Service, U. S. Department of Commerce
5825 Port Royal Road, Springfield, Virginia 22151

Price: Printed Copy $ 4.00 ; Microfiche $3.00

AGNS
Allied-General Nuclear Services

AGNS-35900-CONF-121

Distribution
Category UC-83 Special

AUTOMATED SYSTEM FOR CONTROLLING AUTHORIZATION, IDENTIFICATION, AND ENTRY INTO NUCLEAR FACILITIES

Lawrence D. Barnes

January 1981

For Presentation at 1981 Carnahan Conference
on Crime Counter Measures
Lexington, Kentucky
May 13, 1981

ALLIED-GENERAL NUCLEAR SERVICES
POST OFFICE BOX 847
BARNWELL, SOUTH CAROLINA 29812

PREPARED FOR THE
DEPARTMENT OF ENERGY
WASTE AND FUEL CYCLE TECHNOLOGY OFFICE
UNDER CONTRACT DE-AC09-78ET35900

AUTOMATED SYSTEM FOR CONTROLLING AUTHORIZATION, IDENTIFICATION, AND ENTRY INTO NUCLEAR FACILITIES

by

Lawrence D. Barnes
Allied-General Nuclear Services
Barnwell, South Carolina 29812

Abstract. An automated access control system developed under contract to the Department of Energy at the Barnwell Nuclear Fuel Plant is described. This system enables the facility management to control who has access to sensitive areas at specific times, control the authority to grant access to individuals with cross-checks and verification, and provide positive identification of personnel obtaining entry, as well as an auditable record of all entry events.

The individual seeking access enters his memorized identification number into a key pad in the entry booth. Positive verification of the identity claimed is obtained by a voice verification system which compares the sample response obtained at the time of entry with the individual's voice print reference file. The identified user is then issued a temporary proximity card key which will activate the door entry controls into authorized areas. The computerized system provides real-time entry inventory of personnel and controls individual area and personnel authorizations on a need-to-enter basis.

The system was installed in 1979 and has been operated on a developmental basis since that time. The system controls access to an industrial area which has a total of fourteen (14) separate and individually controlled subareas containing a combined total of twenty-four (24) doors. Approximately five-hundred (500) people are currently enrolled and using the system. Extended tests requiring 100% participation by employees are currently in progress.

INTRODUCTION

The Advanced Physical Protection System (APPS) developed under contract to the Department of Energy by Allied-General Nuclear Services (AGNS) at the Barnwell Nuclear Fuel Plant (BNFP) includes an automated method for the control and monitoring of personnel movement throughout the site. These automated features provide strict enforcement of personnel access policy without routine patrol officer involvement. The system, therefore, allows the patrol force manpower to be utilized more effectively in the monitoring and surveillance functions of physical security.

The primary justification for real-time access control is to comply with anticipated site personnel control requirements for positive identification, control of authorization for entry that is based on current schedules, and to provide a record of who had access. The features pertinent to access control were reported in "Integration and Coordination of Safety-Operations-Safeguards," September 1978[1] and in "Advanced Physical Protection Systems for Nuclear Fuel Reprocessing Facilities," October 1978.[2]

The basic concept was a layered approach to physical barriers. The outermost layer of physical security is the entrance to the Industrial Security Area, and the innermost layers are entrances to the Material Access Areas. Proceeding through the layers of physical security, the requirements for control point passage become increasingly rigid. The various levels of access criteria and the multiple barrier systems mandate the use of automated equipment to provide a consistent and rapid enforcement of these criteria. These multiple control points through the layered barrier system are a key element of the identification and control of personnel throughout the complex. The identification of personnel coincides with the access criteria of the various layers. Identification methods include identification by employee ID number, identification by voice verification, and identification by physical security officer verification. The association of an employee with a proximity card key is another key element in the system. This association is temporary and entirely random. Thus, duplication of the card key would not guarantee access to the plant site.

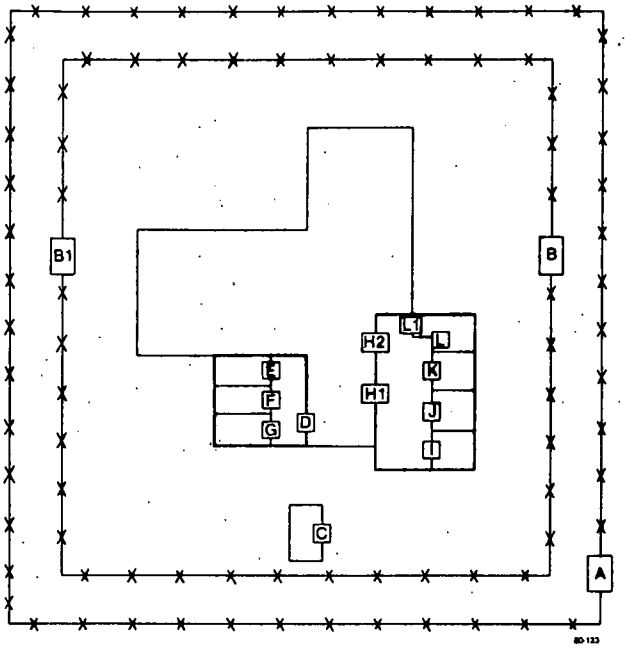
ACCESS CONTROL DEVELOPMENT SYSTEM DESCRIPTION

I. Physical Layout

Access Control System components were installed at various locations throughout the plant site. Figure 1 is an overview showing the relative locations of the major system components that were installed for test and development purposes. The hub of the system is the Safeguards Coordination Center (SCC) shown as Area C in Figure 1. It contains the computers and much of the peripheral equipment necessary for such a system.

A. Industrial Security Area (ISA) Control Point

The ISA control point is the point of initial entry into the safeguarded system. For the internal control system to function properly, the initial employee-card key association must be reliably and accurately controlled. The ISA control point contains the three entry booths,



A	Industrial Security Gatehouse
B	Protected Area Secure Passageway
B1	Protected Area Vehicle Access Passage
C	Safeguards Coordination Center
D	PNSL High Security Manned Portal
E	PNSL Control Room
F	PNSL Upper Level
G	PNSL Lower Level
H1	HCLA Lower Level
H2	HCLA Upper Level
I	Radiochemistry Lab
J	Gas Analysis Lab
K	Pu Product Lab
L	Alpha Lab Lower Level
L1	Alpha Lab Upper Level

Figure 1. Plot Plan of Access Control Test Areas

the voice verification system, the security officer terminal, and the exit turnstiles as shown in Figure 2.

(1) Entry Booth

At the ISA control point, there are three identical booths to perform the employee-card key association. Each entry booth is equipped with a Digital Equipment Corp. (DEC) data terminal, a voice system microphone/speaker assembly, a set of indicator lights, a card key sensor, and an intercom station as shown in Figure 3. The operating sequence developed for entry requires the individual to enter the booth and input his employee identification number at the data terminal. If the employee identification number is accepted and if the employee is enrolled in the voice system, the employee will then be prompted by the voice system described below. If the individual needs assistance, the intercom station may be used to communicate with a security officer. This sequence is shown in Figure 4.

(2) The Voice Verification Access Control (VVAC) Interface

The Voice Verification System is a three-portal system. The communication interface between the VVAC and the DEC Computer (CPU) is through a full-duplex serial data link. Communication between the two systems operates in a master/slave relationship with the DEC CPU serving as the master. All message sequences are initiated by the CPU. The possible message sequences include voice verification, voice enrollment, user deletion, user name modification, and phrase recitation. Voice verification, done for employee-card key association, consists of the VVAC system speaking a verification phrase and the individual repeating that phrase. The VVAC sends a status code to the CPU indicating the results of the requested message sequence.

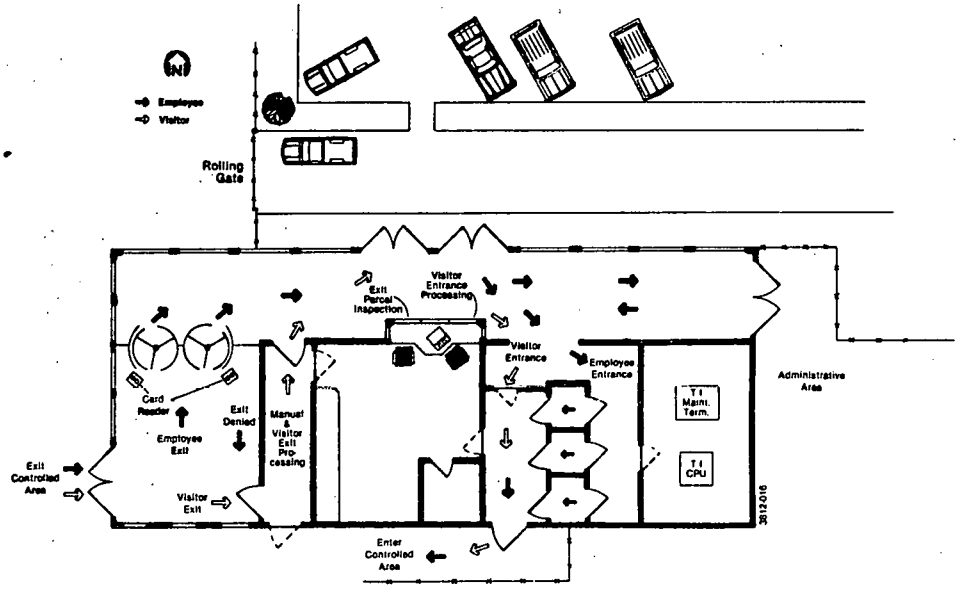


Figure 2. Industrial Security Gatehouse Arrangement

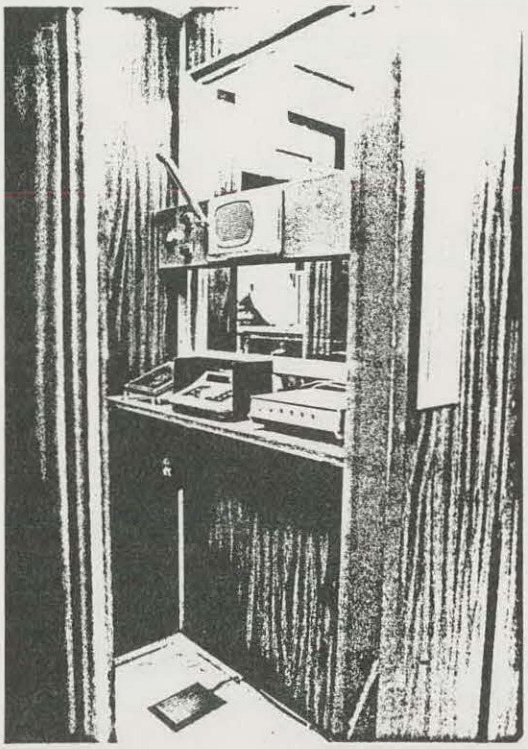


Figure 3. Voice Verification Entrance Control Booth

(3) The Security Officer Terminal

The security officer terminal area allows the security officers to operate the access system. This area includes a VT-100 video terminal and a DEC (Model LA-120) terminal which is used to log events. Figure 5 shows the security officer terminal area.

The video terminal allows the security officers to operate programs designed for the access system. The programs allow the security officers to locate an individual by name, employee number, or area location; to list all individuals who are still in the system at the end of the day; to list all visitors and escorts; and, to manually update an individual's area inventory.

(4) The Exit Turnstile

The addition of the exit turnstile permits controlled egress and card key capture. The exit turnstile consists of two single-person turnstiles and the interface electronics as shown in Figure 6.

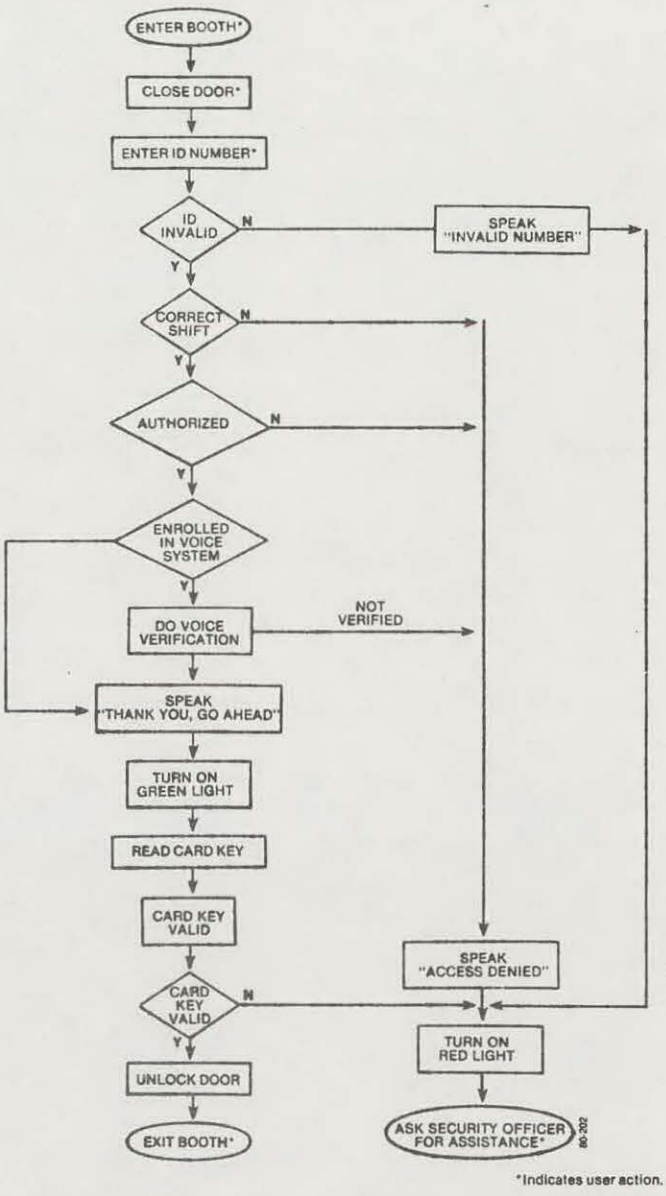


Figure 4. ISA Entry Booth Functional Flowchart

Figure 5. Security Officer Operating Terminal

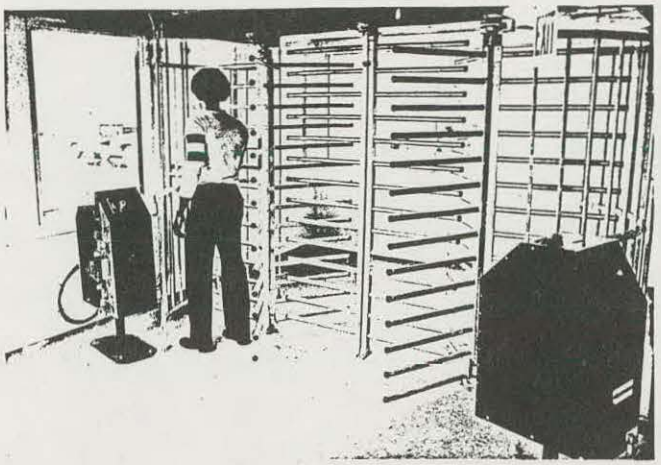


Figure 6. ISA Exit Turnstiles

B. Protected Area Personnel Control Point (SAP)

The Secure Access Passageway (SAP) is included in the access test to represent a manned portal with high security/high traffic flow. The SAP consists of two unmanned access control points with a search zone between them. The entrance door to the SAP must first be accessed by the individual. When the card key is presented at the entrance door, the CPU verifies the individual's authorizations and the individual's inventory status. If the individual is authorized for entry and the individual is inventoried in the ISA, the entrance is released to permit entry. The individual then proceeds through a physical search for contraband (none is performed at this time). The individual must then request portal exit by presenting his card key at the exit door sensor.

C. Protected Area Vehicle Control Point (VAP)

The access test includes provisions for the control of the movement of personnel and material into the protected area by vehicles. The control point for this purpose is the Vehicle Access Portal (VAP). The VAP is a physical search point for the entry of vehicles and includes the facilities for the physical search of vehicles ranging from automobiles to railroad cars.

D. Vital Area Access Control Point

The entrance to a vital area access control point requires control and limitation but does not require a physical search. The demonstration site selected to represent a vital area access control point is the entrance to the SCC. The card key sensor, the indicator lights, and the electric lock are installed on a man-gate in an eight-foot chain-link fence surrounding the entrance to the Safeguards Coordination Center (SCC).

E. Material Access Area Control Point

The Plutonium Nitrate Storage and Loadout (PNSL) facility represents a typical high security/low traffic control point. The PNSL portal consists of two unmanned access control points with a search zone between them. Verification of assignments and identification are performed to maintain tight control. There is a DEC RT-800 data terminal for the use of a security officer for this purpose. The hardware configuration of the PNSL portal is shown in Figure 7.

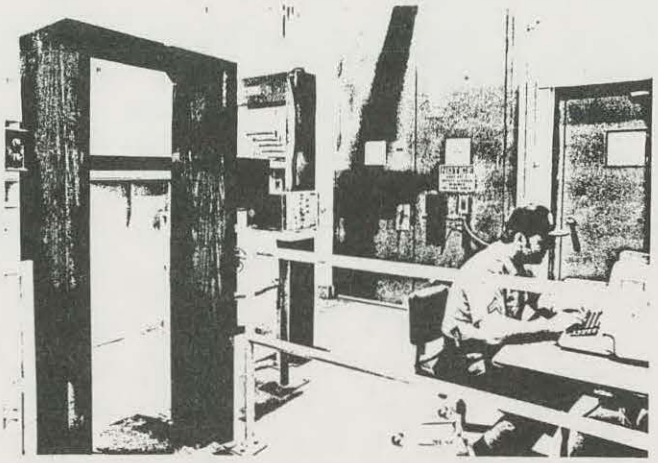


Figure 7. Material Access Area Manned Personnel Search Portal

F. Additional Control Points

The vital area access control was expanded by adding the Hot and Cold Laboratory Area (HCLA) to the access test. To accomplish this, two Schlage proximity controllers were added. A typical HCLA portal contains a proximity sensor, green and red indicator lights, and a magnetic lock. The HCLA is subdivided into the radiation chemical lab, the gas analysis lab, the plutonium product lab, and the alpha lab. The personnel access authorization to the labs is separate to allow access to only specific labs. The operation of the HCLA portals is the same as the operation of the vital area access portal except that the magnetic lock is released instead of the electric lock.

II. Computer System Hardware

The computers selected are Digital Equipment Corporation (DEC) PDP11/34's. The hardware configuration is shown in Figure 8. The primary applications of the computer units are: (1) Communications-Access Control (COM) which controls door opening, indicator lights, card readers, voice verification, etc., (2) Management Information Unit (MIU) which provides a Personnel Access Information Data Base to control access authorization and an event log data base to archive personnel movement, and (3) Zone Operations Control (ZOC) which is another functional system that backs up the COM unit if it fails. A detailed discussion of the hardware is contained in prior reports.(3)

III. Functional Description

The Access Control System is designed to be operated by the Physical Security Patrol Force with a minimum of intensive training. The automation provides a high degree of personnel

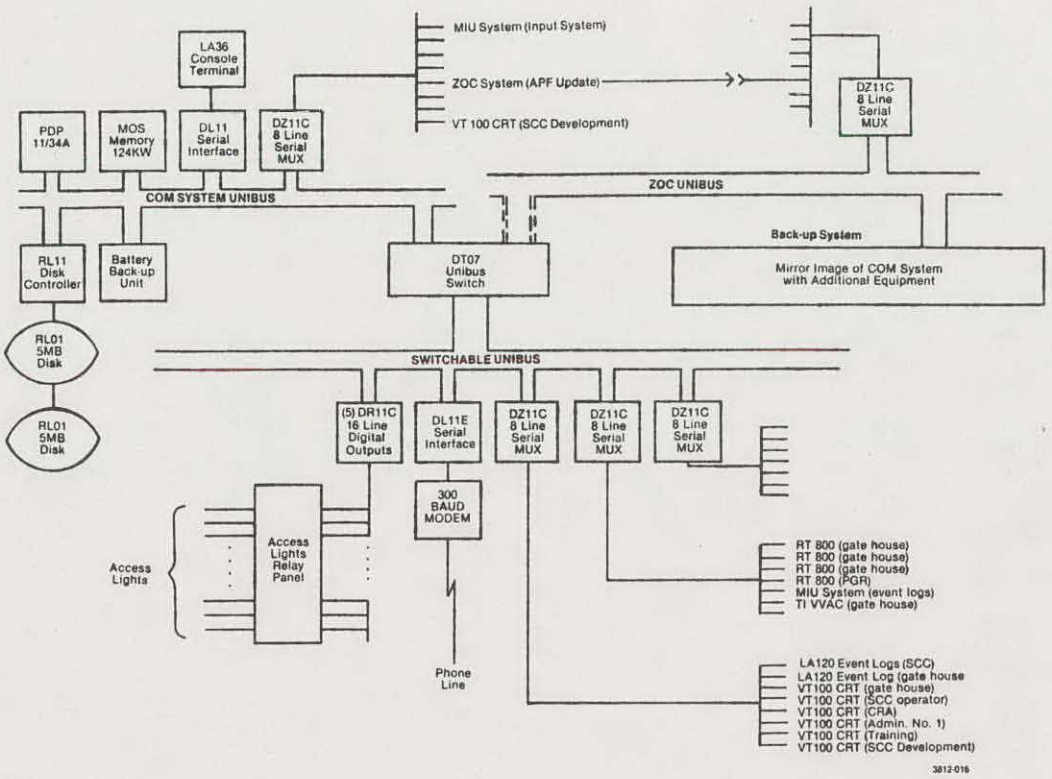


Figure 8. Access Control System Block Diagram

control without requiring significant operating manpower. The Access Control Computer is programmed to provide the following routine physical security checks without specific patrol officer intervention:

(1) Positive Personnel Identification - At the entry point to the controlled area each individual's identity is verified by voice print analysis. The individual's identity is then registered to a card key.

(2) Access Authorization - As the individual's identity is associated with a particular card key signal, the individual's authorization file is checked to verify that; (a) the individual has been administratively approved for entry into the controlled area; (b) the individual's shift assignment is checked to ascertain that a scheduled entry is being requested; and (c) the record of the individual's location within the controlled area is searched to verify that the individual is not recorded inside the controlled area.

(3) Interior Authorization Checks - As individuals present the card keys to request access into controlled areas, the program identifies the individual by the card key signal and verifies; (a) that the individual has administrative approval for passage through the particular control point; (b) the individual is recorded in an adjacent control area; and (c) the area into which passage has been requested is not restricted by an administrative decision.

(4) Access Event Log - The automated system retains a record of each access request generated within the system. The computer files the time, date, individuals's identity, the description of the access requested, and the action taken by the system. In the event of an access denial decision, the cause of this decision is recorded. This information is available to the patrol officers and safeguards operators for evaluation and correction of access problems.

The automated access control not only provides an efficient tool for the Physical Security Force but also incorporates the concerns of the Advanced Safeguards Concepts into the physical protection function. The ability to grant each level of access authority is distributed over the organization so that no one point in the system can make the access control mechanism vulnerable to fraud or sabotage. A prime safeguards objective of access control is to prevent any single individual at any level in the organization from being capable of issuing an authorization for entry into a sensitive or material access area. The access control system is designed such that input from multiple departments within the organization is required before an individual will be recognized to have access authority. A sequence of input data from the various organizational departments is held in the file and screened by an on-line real-time authorization generation program. The input components required for a specific level of access authority must be present (as data entered into real-time authorization file created by the screening program),

before access will be granted by the automated system.

The safeguards objective of documenting the movement of personnel into and out of vital and material access areas is well served by the Automated Access Control System. Each event, beginning with entry into the controlled area and continuing until the control area exit, is recorded and stored by the computer system. The data including date, time, individual identity, description of the access request, and description of the programmed decision with a cause of each access denial is retained in the computer file for a specified working period and then transferred for permanent storage on computer readable media.

The existence in the computer of the access event data gives occasion to generate programs to provide further benefits for the Physical Security Force, Operations Department, Safety and Health Physics Department, and the Safeguards Department. The access data provides basis for a personnel accountability or personnel inventory feature. Each access event results in the specific individual being recorded as an occupant of the controlled area. As access events occur, the inventory of both the entered and the exited control area is updated so that a current inventory is always available for display. The display capability is provided to all terminal locations to make this information available to all involved organizational departments. The inventory display is an instantaneous listing of personnel location. The information is made available for situation assessment and not as a surveillance and monitoring tool. Personnel location can be determined by entering the individual's name or employee number. By entering the identification of an individual, the area in which that individual is recorded will be displayed. By entering a specific control area identification, a listing is displayed of all individuals recorded in that particular control area.

The processing and display of the information from the access control system not only has practical value to the organizational departments, but also promotes user acceptance. The acceptance of the system by the patrol officers, the production supervisors, and the safety-health physics technicians contributes significantly to the effort to integrate an Advanced Physical Protection and Safeguards system into the established operations-oriented organization.

Summary of Results

The development program demonstrated that the total system could be operated in an integrated manner and effectively control entry and exit from controlled areas at normal throughput levels without causing significant personnel delays. Event log reports were demonstrated that proved the system's ability to track individuals, record all access events, and display unauthorized entry attempts as required. The rapid alteration of individual data base files was demonstrated. The system proved of value to Physical Security for effectively maintaining authorization files, updating files, listing current status on all employees, and listing status of contract personnel holding access credentials. Files on about 500 people, who are authorized to enter the ISA without escort, are contained on the system.

Multiple portal operation of the voice verification system verified that a single host CPU could handle three portals effectively without a significant degradation of processing time for each access attempt. Approximately 250 people were successfully enrolled on the VVAC system, and only two people have been identified that could not be enrolled because of identified handicaps.

Typical access control pattern and throughput were handled successfully. They involved approximately 400 entries and 400 exits to ISA and approximately 2000 door openings or access events within the facility per 24 hours.

References

1. Barnes, L. D., et.al., Integration and Coordination of Safety-Operations-Safeguards, AGNS-1040-2.3-44 (September 1978).

2. Barnes, L. D., et.al., Advanced Physical Protection Systems for Nuclear Fuel Reprocessing Facilities, AGNS-1040-2.3-45 (October 1978).

3. Collert, G. T., et.al., Automated Personnel Identification and Access Door Control, AGNS-35900-2.1-109 (November 1980).

DISTRIBUTION FOR CONFERENCE PAPER NO. AGNS-35900-CONF-121

AUTOMATED SYSTEM FOR CONTROLLING AUTHORIZATION, IDENTIFICATION, AND ENTRY INTO NUCLEAR FACILITIES

AGNS Internal Distribution:

K. J. Bambas (1)
L. D. Barnes (1)
P. E. Ebel (1)
J. H. Ellis (1)
J. A. Gibbons (1)
W. Knox (1)
A. A. Moultrie (1)
E. L. Musselwhite (1)
R. L. Postles (1)
J. K. Shaffer (1)
J. C. Smith (1)
Records Management (18)

DOE Distribution:

Mr. J. W. Geiger, Project Engineer (1)
Waste and Fuel Cycle Technology Office
DOE Savannah River Operations Office
Post Office Box A
Aiken, South Carolina 29801

Dr. J. Spencer (1)
Savannah River Laboratory
E. I. du Pont de Nemours & Company
Aiken, South Carolina 29801

Mr. William Burch (1)
Oak Ridge National Laboratory
Post Office Box X
Oak Ridge, Tennessee 37830

Mr. S. W. O'Rear, TIS (1)
Savannah River Laboratory
E. I. du Pont de Nemours & Company
Aiken, South Carolina 29801

Mr. A. F. Westerdahl (1)
Patent Counsel
DOE Savannah River Operations Office
Post Office Box A
Aiken, South Carolina 29801

Mr. D. C. Drennon (1)
Contracting Officer
DOE Savannah River Operations Office
Post Office Box A
Aiken, South Carolina 29801

Mr. J. M. Bauer, Jr. (1)
Classification Officer
DOE Savannah River Operations Office
Post Office Box A
Aiken, South Carolina 29801

Mr. W. W. Ballard (1)
Acting Director
Nuclear Fuel Cycle Division
Office of Light Water Reactors
DOE Germantown, Maryland 20767

Mr. M. J. Lawrence (1)
Acting Director
Office of Transportation and Fuel Storage
Nuclear Waste Management Program
DOE Germantown, Maryland 20767

TIC Distribution:

DOE Technical Information Center (2)
Post Office Box 62
Oak Ridge, Tennessee 37830