CONF-950787--10

SAND95-1298C

INTEGRATION OF ACCESS CONTROL AND ANCILLARY INFORMATION SYSTEMS

J. R. Rodriguez
Sandia National Laboratories
Albuquerque, New Mexico USA

J. S. Ahrens
Sandia National Laboratories
Albuquerque, New Mexico USA

ABSTRACT

The DOE has identified the Lawrence Livermore National Laboratory ARGUS system as the standard entry control system for the DOE Complex. ARGUS integrates several key functions, specifically, badging, entry control, and verification of clearance status. Not all sites need or can afford an ARGUS system. Such sites are therefore limited to commercial equipment which provide ARGUS like features. In this project an alternative way to integrate commercial equipment into an integrated system to include badging, access control, property control, and automated verification of clearance status has been investigated. Such a system would provide smaller sites the same functionality as is provided by ARGUS. Further, it would allow sites to fully participate in the DOE's concept of Complex wide access control.

This multi-year task is comprised of three phases. Phase 1, system requirements and definitions, and phase 2, software and hardware development, were completed during fiscal year 1994. This report covers these two phases and the demonstration system which resulted. Phase three would employ the demonstration system to evaluate system performance, identify operational limits and to integrate additional features. *(The status of this phase will also be presented)*

The demonstration system includes a badging station, a database server, a manager's workstation, an entry control system, and a property protection system. The functions have been integrated through the use of custom interfaces and operator screens which greatly increase ease of use.

1.0 System Overview

As shown in Figure 1, the system is comprised of four stations. Each station is a dedicated PC with the exception of the Entry/Property Control system which uses a PC for each function. The stations are all connected together via an Ethernet network. Two custom operator interfaces were written for the system. The first is the Manager Application which runs on the Manager's station. It accepts user input and updates the central database on the Network Server. The second is the Entry Control/Badging application. This application runs on the Badging station and its purpose is to provide a controlled access point to the badging and biometric equipment. This application also writes to a shared file which is used to communicate with the Entry Control system. The following sections provide greater detail of the system.

Requirements and specifications were determined through a series of meetings and conversations between the project staff, software support staff and management. Software support was contracted to Science and Engineering Associates (SEA). In order to evaluate the effectiveness of distributed databases it was necessary to develop a multiple node network on which to test our assumptions. The network developed is based on Microsoft's Windows for Workgroups. The network includes a commercial badging station, a database server, a manager's workstation, and an entry control monitoring station. The functions have been integrated through the use of custom front end operator screens which greatly increase ease of use. A diagram of the network is shown in Figure 1.

This work was supported by the United States Department of Energy under Contract DE-AC04-94AL85000.

DISCLAIMER

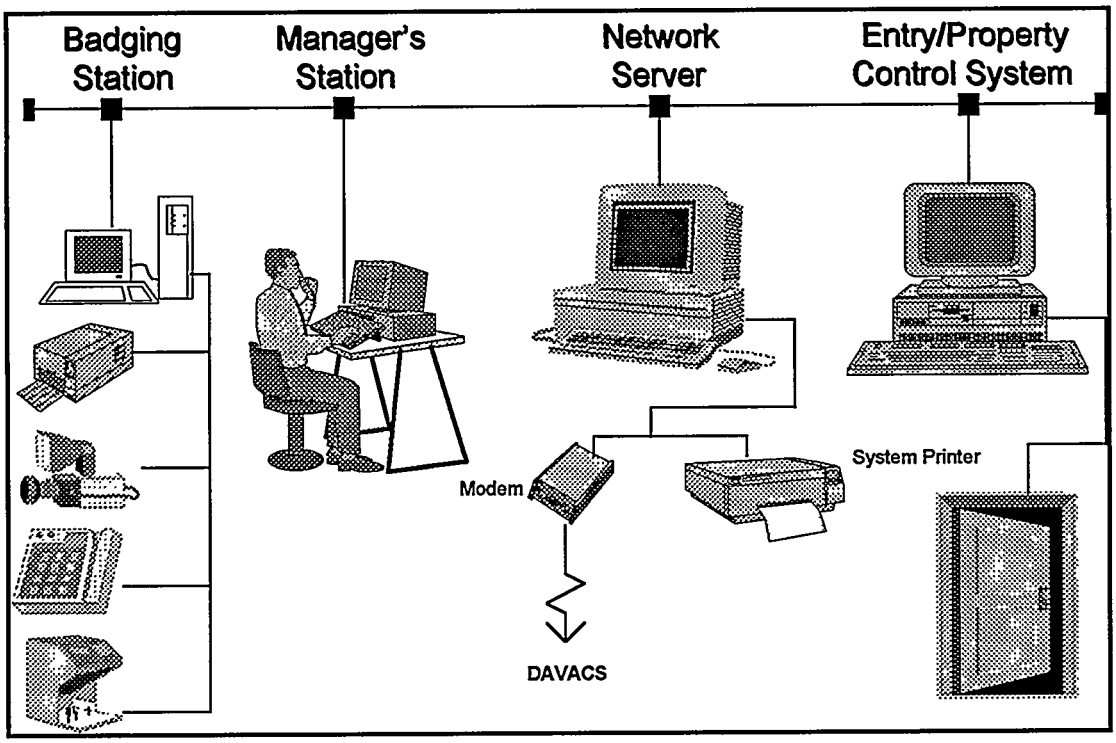

Figure 1

2.0 Manager's Workstation

The full name of the manager's workstation is Security Manager/User Administration workstation. It is at this station that user information is first entered and later updated. This station is comprised of a DOS 6.2 computer running Windows for Workgroups. The computer has an integrated Ethernet interface and so no additional hardware was required. This station runs a database access manager called SEAVIEW. SEAVIEW allows queries and updates to the database through SQL commands which can easily be constructed through point and click mouse commands.

To create a new user, the administrator first clears the data entry screen, Figure 2, by clicking on the NEW button. The following information may then be entered:

> Last name, First name, Middle name, Social Security number, Site code, User type, Special access letters, Sigma, Restrictions, Begin date, and End date.

After this information is entered the administrator clicks the Ready for Badge Making button. A verification is made to ensure the user is not currently in the database. If a duplicate social security number is found a message is returned to the administrator. Otherwise, a badge number is assigned and a separate task is launched which checks the DOE DAVACS system to verify clearance level. Currently this task is not implemented and so always returns true. At the time of development the DOE system was being redesigned by LLNL. In the future, the new system (DISS-DOE Integrated Security System), will be queried at this point.

After these checks a flag is set in the database indicating the badge is ready for issue. The badge number is modeled after the version of the DOE Standard Security Badge Manual which was current at the time these task requirements were fixed. It was recognized that since that manual had not been officially adopted, there was a chance changes would be made.

Badge numbers are sequentially assigned depending on the type of user (see Table 1). It is not possible for an administrator to assign a badge number or type in an issue date without following this procedure. The fields assigned to the Badge area of the data entry form are non-modifiable.

User Type	Clearance Level "Q"	"L"	None
SNL Employee	A	B	C
Contractor	D	E	F
DOE Federal	G	H	I
DOE Other	J	K	L
Other Federal	M	N	O
Other	P	Q	R

Table 1

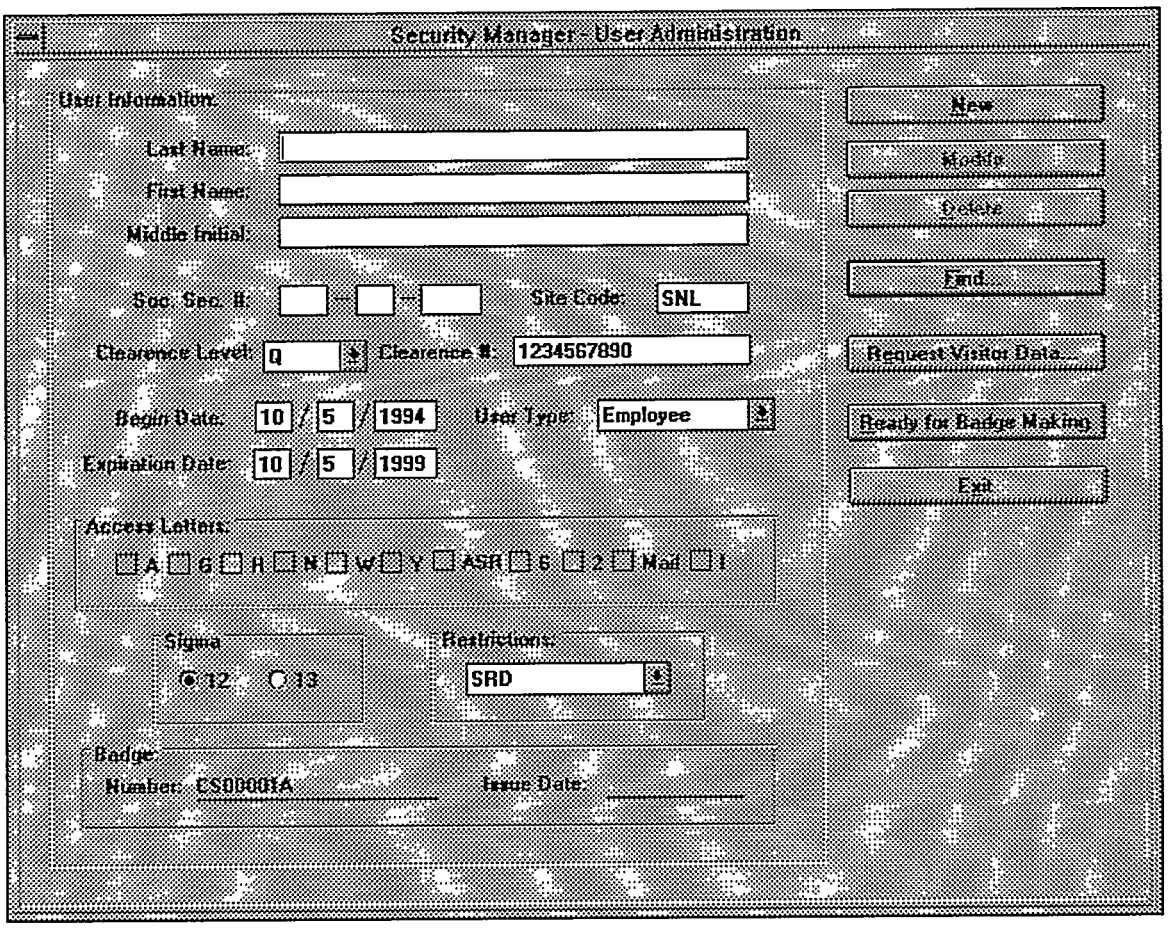

Figure 2

Command Button	
New	This button clears any existing information from the screen.
Modify	The Modify button updates the data in the database with what is shown on the screen for the specified user. This gives the System Administrator the ability to change begin and expiration dates.
Delete	The Delete button, deletes the specified user from the database and issues a delete message to the Entry Control Server.

Find	The Find button searches for the user information specified by the Social Security Number.
Request Visitor Data	This button imports clearance level information from the DOE DISS system. This feature is currently not implemented.
Ready for Badge Making	This button launches a check against the DOE clearance database (currently not implemented) and upon verifying clearance level, a badge number is issued and a flag is set in the database which authorizes the creation of a badge.
Exit	The Exit button closes the application. Note that a password may be required to restart the application.

The Badge number begins with a fixed code "CS" which identifies SNL as the issuer. The next five numeric characters are the sequencial number. The user type from Table 1 above is at the end. An example badge number of a "Q" cleared, DOE contractor would be: CS12345J.

Once all the above steps are successfully accomplished the user may go to the badging station for badging.

The manager also has, outside of the manager's application, a SEAVIEW client. This windows program provides easy access to the database for both ad hoc queries and daily transaction processing. SEAVIEW enables the manager to view, print and manage documents, images and audio files. Database queries can be built and saved for future use.

3.0 Badging Station

The badging station is a DataCard badging system. The system is a commercial product which includes a computer terminal, a direct print-on-plastic printer, a CCD camera for image capture, and integrated software. The software supports card design, database design, and card production. For a detailed description of the system see *Evaluation of the QuickWorks Image Capture Station*[1]. This system was augmented with a 3Comm network card and an additional serial port. Three Windows programs were also added. One to control a magnetic stripe reader/writer, another to control a Recognition Systems ID3D hand geometry identity verifier and a third which is the operator's interface. This third application launches all others and manages the communications between database server and other system elements.

When a user arrives at the badging station, the operator asks for a social security number and uses the Find button to retrieve the individual's record from the database. The operator is required to validate the user's identity (i.e., ask for driver's license or other picture ID). The Create Badge, Acquire Biometric and Encode Magnetic Stripe buttons will be enabled to begin the badging process. Only when the three aforementioned processes are complete, will the Badge Making Done button be enabled. If the button remains gray a problem was encountered and the operator should have the Security Administrator check the clearance status.

After completion of a successful badge making process, the badging application returns to the database the biometric template, the image file and the database status field will be changed to 'issued'. The application also passes to the Entry Control server the social security number, biometric template, and expiration date.

The newly enrolled person's biometric template and possibly picture would then be sent up to the DOE DISS system so that the master database may be updated. There currently does not exist an automated method for updating clearance records therefore this feature was not implemented.

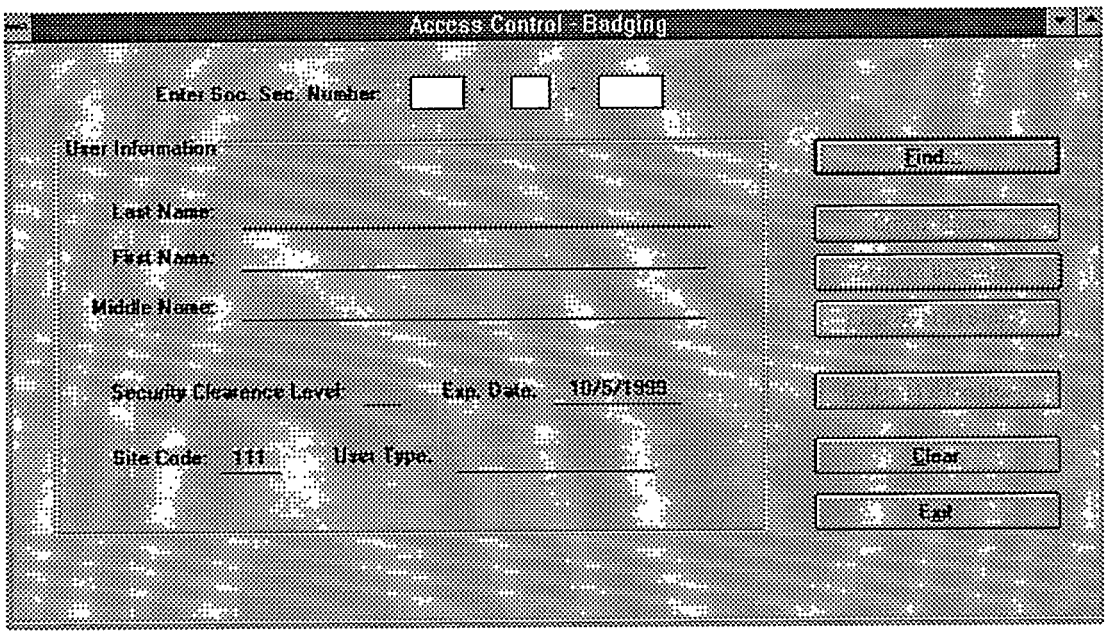

Figure 3

Command Button	
Create Badge	This button launches the DataCard application if the user is found in the database. If not found or the social security number is invalid, a message box is displayed. When the badge is created and the DataCard application is closed, the focus is returned to the Access Control-Badging application.
Acquire Biometric	This button launches the Hand Geometry application to capture the user's hand geometry. When this process is complete, the focus is returned to the Access Control-Badging application.
Encode Mag Stripe	This button launches the application to ask for and to perform the encryption of the PIN. It also encodes track 2 of the security badge in accordance with the specifications in the DOE Standard Security Badge Manual.
Badge Making Done	The Badge Making Done button is grayed until Create Badge, Acquire Biometric and, the Encode processes are successful. This button collects necessary data and down loads it to the shared directory in a response file. The badge issue date, photo, PIN and hand geometry information are also inserted into the data base. The create badge authorization flag is reset. If the photo, hand geometry data or PIN encryption fails, a message box indicating the error is displayed.
Exit	The Exit button closes the application. Note that a password may be required to restart the application.

4.0 Entry Control Communication Application

The Entry Control (EC) Communication application was written in C. It resides in the Administrator's work station. This application runs at all times and polls for the request files from the shared directory. The purpose of this application is to communicate with the entry control system which is a dedicated DOS application and to ensure the database and entry control server data remain synchronized. The EC Communication application acknowledges the system's requests by reading the request files from the shared directory. It responds in one of two ways depending on the

request. If the request is for information about an unknown person requesting access at an entry control point, a response file containing the requested user information is generated. The second form is for updating the central database with a new biometric template of an existing user. This form is used to update all entry control points when the biometric feature changes.

5.0 EC Communication Files Description

There are two types of files that may reside in the shared directory on the Admin server. Both files have the same file format. The files are written in ASCII and in Token Layout. Data includes user ID (social security number), expiration date, hand geometry template in HEX and, a Add / Delete / Update flag, set to 1, 2, or 3 respectively. The types of files are:

Request File

- Random filename with extension ECQ
- EC system produces request file whenever it is necessary to retrieve user information from the database.
- EC system creates a request file with an update status flag, when it encounters a biometric template which has changed sufficiently from the one stored in the database. The update file contains the new biometric template. It is intended that this new template will trickle up to the DOE DISS system, once that system is available.

Response File

- Random file name with extension ECD
- Error indicator format in addition to data format
- EC communication application creates a response file when it receives the request file. The response file contains the information queried by the request file. If the requested user is invalid, an error statement is written out to the response file instead of the requested user information.
- A response file is also written whenever a user is removed from the database and further access is denied.
- The Access Control application creates a response file when the operator presses the Badge Making Done button. This response file contains the social security number, the hand geometry template in hexadecimal notation, and the add flag set to true.

6.0 Database Server

The database server is a DOS 6.2 computer. It contains a 3Comm network interface board and associated software drivers. The database engine is Gupta Technologies' SQLBase version 5.1.4. The data management software is Science and Engineering Associates' SEAVIEW.

Database Server

Processing duties are shared between the client and server. The client takes user input and submits requests to the server. Database processing, such as retrieving and sorting, is centralized at the database server. Application processing is distributed between the server and the clients. The server only sends the parts (subsets) of the database requested. An SQL database server was selected because of SQL's convenient language for specifying logical subsets of data and because both the American National Standards Institute (ANSI) and the International Organization for Standardization (ISO) are developing SQL as a standard interface to a relational database management system.

SEAVIEW Client

The SEAVIEW client organizes information into Cabinets, Drawers, Folders and sub folders. It provides the architecture for the application programs to interface to the database server. The most important feature of SEAVIEW is its ability to work with images, such as the pictures of users and signatures. With this feature it would be very easy to add an additional computer to the system which takes a social security number as input and presents the picture, signature and other information about the owner. Such an application would work well at manned entry control points such as front lobbies where security personnel can check the claimed identity of persons not having the correct credentials.

7.0 Conclusions

Commercial equipment has been integrated into a multi-function system. The ability to join existing equipment and databases has been demonstrated. The potential value of such system integration is promising and should be better quantified in future years. The technical problems of changing biometric templates and of transmitting templates between sites are not insurmountable. As the issues are identified, solutions may then be found. This system allows for future study directed at identifying problem areas and providing engineered solutions.

---

[1] Grant Wells and Jose Rodriguez, Laboratory Report: Evaluation of the QuickWorks Image Capture Station, Sept. 1994.