Requirements Spec for the Personnel Access Control System (PACS)

1. Introduction: Purpose and Background

The purpose of this specification is to provide sufficient detail to the software team to design, develop, test, and integrate the software system into the Personnel Access Control System (PACS).

2. System Overview

a. System Concept

The PACS system is a simplified version of an automated personnel entry access system (gate) used to provide privileged physical access to rooms/buildings, etc. A user inserts his personal I.D. card which contains his/her name and social security number into a reader. The system searches for a match in the software system database which may be periodically updated by system administration, instructs/disallows the user to enter his/her personal identification number (PIN), a 4 digit code using a display attached to a simple 12-position keyboard, validates/invalidates the code, and instructs/disallows entry into the room/building through a turnstile gate. A single line display screen provides instructional messages to the user. An attending security officer monitors a duplicate message on his console with override capability.

There are six simple hardware components in the PACS system: the card reader, keyboard, single line digital message display unit, guard reset unit, and gate (see "External Interface" in Section 3).

b. Expected Operational Environment and Reliability

The software system shall be delivered as C or C++ source code (and a listing). For simplicity, the PACS software shall service only one card/badge reader station which shall be assumed to be in operation 24 hours a day, seven days a week. Any failure of the system shall default to an "Access Denied" message to the reader and a message to the attending guard.

System loading will vary from light to heavy depending on the time of day and day of week. A Level 1 failure occurs when the software is hung, valid user cards and valid PINs are not processed, invalid users have access, or the guard cannot override the system. In summary, a Level 1 failure is one which leads to a non-functioning system. The reliability target shall be 0.99 per transaction (i.e., 99 of 100 transactions shall run without a Level 1 failure).

A Level 2 failure, on the other hand, is a non-critical failure. The guard can override these non-critical malfunctions and still keep the system running. Level 2 system failures include anomalies, such as a user with a large package who needs extra passage time. A Level 2 failure has an operational work-around. The target reliability shall be 0.9 per transaction for Level 2 failures.

A Level 3 failure is a "Don't Care" failure which will be fixed on the next release of the software. An example of a Level 3 failure is a documentation error.

c. Overview of high level design

The software system shall display the message, "INSERT CARD" and then check for success (1 in R6) or failure (0 in R6) once the card has been entered into the reader. In the case of successful card entry, the system shall read the nine-digit social security number and the last name which can contain up to 20 characters. Validation shall be done against the file called Card.val. If the data is valid, the software shall update the 20 ASCII digit LED file called message.led with "Enter PIN". If the card is unreadable, then a message "Retry" shall be posted to the LED file for a maximum of three tries. After the third failure, the system shall post to the LED file "See Officer". A duplicate message is sent to the officer by the software to the file Officer.led and register 8 is set with a value of 1. The officer must reset the PACS software system before operation of the system can proceed and does so by setting register 7 with a 1. The software system shall read this register and re-initialize. The 4-digit PIN shall be read from keyboard register R1 through R4 and compared against data in Card.val file. Note, the first digit is stored in Register 1, the second digit in Register 2, etc. The software shall allow a maximum of 5 seconds between digits before the "Invalid PIN" message is displayed. Once a PIN value has been entered and failed for three tries, a "See Officer" message is sent to file called Officer.led and also displayed on the keyboard's LED using the message.led file. A valid PIN should generate the message "Please Proceed" to the user after a flag is set to 1 in Register R5 upon which the hardware opens the gate. After 10 seconds, the system automatically resets itself for another entrant or after an entrant has passed through the gate successfully.

3. Requirements (Software)

a. Functional Requirements

1. Read date from entrant's card and validate card data.
2. Report and record successes and failures of entrants.
3. Read and validate keyboard input PIN values.
4. Record and report successes and failures for PIN data.
5. Control the opening and closing of the gate depending on validation.

b. Performance requirements.

1. The software shall read keystrokes as quickly as typed.
2. Data validation and message display shall take less than 1 second.

c. Security Requirements

1. The software system shall maintain an audit log on all transactions, both successful and unsuccessful. The purpose of the audit trail is accountability.
2. Any Level 1 or Level 2 system failure shall default to a locked gate but with guard override capability.
3. Any mismatch between database and user entered card or PIN shall:
    a. Display "Inserted card/PIN" for first 3 tries.
    b. Send a message to the guard after the third unsuccessful try and wait for the guard to reset the reader or override gating.

d. Design Constraints

1. The database of users is limited to 1000 triples of SSNs, names, and PINs.
2. For simplicity, there shall be only one card reader/keyboard/gate combination being serviced at a time by the software.
3. The card reader, keyboard, and display are all one unit. The keyboard has 12 keys: 0 through 9 plus # and *; the latter two characters allow the deletion of keystrokes.
4. The entering person shall have five seconds between keystrokes on his PIN; otherwise display: "Invalid PIN".
5. The system shall allow the user a max of 10 seconds between "Enter PIN" and user's first key entry; otherwise, system reset.

e. External Interfaces-user, hw, sw, communication

1. Interface parameters/register-R-minimum two bytes each
    a. Card reader data-parameter ICAR (29)
    b. Keyboard registers for PIN input– R1 through R4.
    c. Officer reset/clear card reader– R7
    d. Officer alert of failed PIN– R8.
    e. Gate control register– R5.
    f. Card in reader – R6.
    g. End of data form card reader – Register R10.
    h. End of PIN data– Register R11.
2. System software utility: clock time for audit file.

f. Other-data base, operations, site-environment

1. Standard keyboard messages (case is unimportant):

   Insert Card

   Re-entry

   Invalid PIN

   See Officer

   Enter PIN

   Please Proceed

   Access Denied

2. Database files and structured description

   card.val – system database of user SSNs, last names, and PINs

   (1000 structures max/1 per each valid entrant with 3 sun-fields)

   SSN integer format – nine integer string

   last name – ASCII character string with maximum length 20

   PIN –integer string of length 4

   Message.led – message buffer for entrant's LED display (fixed ASCII string)

   Officer.led – officer's LED message buffer (fixed ASCII string)

   audit.act – time (system clock) , date, (system), user SSN and name, transaction success/failure (i.e.1 or 0) for each transaction and structure.

4. Project Goals

Produce precise requirements and design documents, build an implementation, and construct and run test cases to evaluate the implementation. Base these on the attached requirements spec.

5. Contact Person

The contact person for this project is Constance Heitmeyer (heitmeyer@itd.nrl.navy.mil).