MOTION CONTROL ENGINEERING, INC.
11380 WHITE ROCK ROAD
RANCHO CORDOVA, CA 95742
TELEPHONE (916) 463-9200 FAX (916) 463-9201

Elevator Security User's Guide

PART # 42-02-S024 REV. B.2 JUNE 2005

TABLE OF CONTENTS

SECTION 1
PRODUCT DESCRIPTIONS

1.0 Introduction 1-1

1.1 Description of Basic Security 1-1

1.3 Description of Basic Security with CRT 1-2

1.4 Description of Access Control for Elevators (ACE) 1-2

1.5 Description of Security Interface Software (SIS) 1-3

1.6 An Overview of MCE's Elevator Security 1-4

SECTION 2
BASIC SECURITY

2.0 General 2-1

2.1 Description 2-1

2.2 Turning Basic Security ON and OFF 2-1

2.3 Viewing and Changing the Security Codes - PTC and PHC 2-3

2.3.1 Viewing the Building Security Menu 2-3
2.3.2 Programming the Security Codes 2-3

2.4 Viewing and Changing the Security Codes - Swing Panel 2-4

SECTION 3
BASIC SECURITY WITH CRT - SWING PANEL

3.0 General 3-1

3.1 Introduction - Product Description 3-1

3.1.1 Main Menu Screen 3-2
3.1.2 Security Menu Screen 3-3
3.1.3 Security Configuration Menu Screen 3-4

3.2 Turning Elevator Security ON and OFF 3-6

3.2.1 Master Software Key Status 3-6
3.2.2 Security Software Switch 3-7
3.2.3 BSI 3-8
3.2.4 Security Configuration Status 3-8

3.3 Using the CRT Terminal to Program the Elevator Security 3-9

3.4 Programming the Security Menu Password 3-9

3.4.1 Changing the Password 3-9
3.4.2 Lost or Forgotten Password 3-10

3.5 Programming the Security Configurations 3-10

3.6 Programming the Security Configuration Timer Table 3-13

3.7 Viewing and Changing the Security Codes 3-14

3.8 Programming Checklist 3-18

SECTION 4
BASIC SECURITY WITH CRT - PTC AND PHC

4.0 General 4-1

4.1 Introduction - Product Description 4-1

4.1.1 Main Menu Screen 4-2
4.1.2 Security Menu Screen 4-3

4.2 Turning Elevator Security ON and OFF 4-5

4.2.1 Master Software Key Status 4-5
4.2.2 Security Software Switch 4-7
4.2.3 BSI 4-7
4.2.4 Security Configuration Status 4-7

4.3 Using the CRT Terminal to Program the Elevator Security 4-9

4.4 Programming the Security Menu Password 4-10

4.4.1 Changing the Password 4-10
4.4.2 Lost or Forgotten Password 4-10

4.5 Programming the Security Configurations 4-11

4.6 Programming the Security Configuration Timer Table 4-12
4.6.1 Programming Instructions 4-13

4.7 Viewing and Changing the Security Codes 4-15

4.7.1 Viewing the Building Security Menu 4-15
4.7.2 Programming the Security Codes 4-15

4.8 Programming Checklist 4-16

SECTION 5
ACCESS CONTROL FOR ELEVATORS (ACE)

5.0 General 5-1

5.1 Introduction - Product Description 5-1

5.1.1 Main Menu Screen 5-3
5.1.2 Security Menu Screen 5-4
5.1.3 Security Configuration Menu Screen 5-5

5.2 Turning ACE Security ON and OFF 5-6

5.2.1 Master Software Key Status 5-6
5.2.2 Security Software Switch 5-8
5.2.3 BSI 5-8
5.2.4 Security Configuration Status 5-9

5.3 Using the CRT to Program ACE Security 5-10

5.4 Programming the ACE Password 5-10

5.4.1 Changing the Password 5-10
5.4.2 Lost or Forgotten Password 5-11

5.5 Programming the Security Configurations 5-11

5.6 Programming the Security Configuration Timer Table 5-14

5.7 Assigning the Passenger Access Codes (PAC) 5-16

5.7.1 Passenger Information Menu Screen 5-17
5.7.2 Changing the PAC Size 5-18
5.7.3 Entering Passenger Information into the PAC Database 5-18

5.8 Programming the Group Time Schedules 5-22

5.8.1 Changing a Group Name 5-24

5.9 Security Reports 5-25

5.9.1 Viewing the Secured Car Call List 5-25
5.9.2 Clearing the Records of Registered Car Calls 5-27
5.9.3 Printing the Secured Car Call Report 5-27

5.10 Programming Checklist 5-27

SECTION 6
SECURITY INTERFACE SOFTWARE (SIS)

6.0 Introduction 6-1

6.1 Getting Started 6-2

6.1.1 System Requirements 6-2
6.1.2 Windows Installation 6-2
6.1.3 CMS Installation 6-2

6.2 Security Job Connection Menu 6-3

6.2.1 Com Port Setup 6-4
6.2.2 Select Com Port 6-5
6.2.3 Specify Baud Rate 6-5
6.2.4 Specify Media 6-7
6.2.5 Specify Phone Number 6-8
6.2.6 Connect to Controller 6-8
6.2.7 Exit 6-9

6.3 Security Interface Software Main Menu 6-10

6.3.1 Basic Security Main Menu 6-10
6.3.2 Access Control for Elevators (ACE) Main Menu 6-11

6.4 Security Configuration Menu 6-12

6.4.1 Security Status - Turning Security ON and OFF 6-12
6.4.2 Program a Security Configuration 6-13
6.4.3 Edit the Security Configuration Timer Table 6-15
6.4.4 Activate a Security Configuration 6-16

6.4.5 Modify the Security Software Switch 6-17
6.4.6 Return to Main Menu 6-17

6.5 Passenger Information Menu 6-18

6.5.1 Modify Passenger Data 6-18
6.5.2 Modify Group Data 6-23
6.5.3 Set Length of Access Codes 6-25
6.5.4 Return to Main Menu 6-25

6.6 Report Generation Menu 6-25

6.6.1 List of Secured Car Calls Registered 6-26
6.6.2 Initialize Controller List 6-26
6.6.3 Initialize Disk File 6-26
6.6.4 Return to Main Menu 6-26

6.7 Change Controller Password 6-27

SECTION 7
SECURITY INTERFACE SOFTWARE (SIS) FOR WINDOWS

7.0 Introduction 7-1

7.1 Getting Started 7-2

7.1.1 System Requirements 7-2
7.1.2 Standalone Installation 7-2
7.1.3 Startup 7-2

7.2 Connection Choices 7-3
7.2.1 Modem Configuration 7-5
7.2.2 Add or Delete Job Setups 7-5

7.3 Controller Menu 7-6
7.3.1 Connecting to a Controller 7-7
7.3.2 Displaying Security Status 7-8
7.3.3 Selecting a Controller Password 7-10
7.3.4 Editing Security Configurations 7-11
7.3.5 Editing Timer Tables 7-16
7.3.6 Setting Configuration Status 7-19
7.3.7 Setting the Security Software Switch 7-21
7.3.8 Entering Passenger Data 7-22
7.3.9 Report Generation Menu 7-29
7.3.10 Disconnecting From a Controller 7-30
7.4 The Help Menu 7-31

APPENDIX

Elevator Security Information and Operation A-1

Index A-5

SECTION 1
PRODUCT DESCRIPTIONS

1.0 INTRODUCTION

Elevator Security is typically used to prevent access to specific floors of a building via the elevators, or to limit access to passengers with a valid password. MCE's elevator security options include:

- Basic Security
- Basic Security with CRT
- Access Control for Elevators (ACE)
- Security Interface Software (SIS)

These elevator security options are implemented on the simplex/duplex Car Controller and/or the Group Supervisor in an M3 Group System. This section provides a description of MCE's Elevator Security options.

1.1 DESCRIPTION OF BASIC SECURITY

Basic Security provides a means to prevent registration of unauthorized car calls. It is implemented on each individual elevator Car Controller. Security codes can be assigned for each floor of a building. The security codes consist of one to eight landing labels and are programmed using the controller's Main Processor board (MC-MP-xx or MC-PCA-xx). Section 2, *Basic Security*, provides instructions for programming the security codes.

Floors for which a security code has been programmed are *secured* when Basic Security is turned ON. In order to gain access to a secured floor via the elevator, the correct security code must be entered using the Car Operating Panel (COP) buttons. When the COP button for a secured floor is pressed, the button's indicator will flash to indicate that a security code is required. The passenger must enter the correct code within 10 seconds, otherwise the call will not be registered and the indicator will turn OFF.

Basic Security is turned ON and OFF using the controller's Building Security Input (BSI). This input can be activated by a switch or external timer.

1.3 DESCRIPTION OF BASIC SECURITY WITH CRT

Basic Security with CRT is an extension of Basic Security, and provides a means to prevent registration of unauthorized car calls and/or hall calls. As with Basic Security, the security codes for each floor are programmed using the controller's Main Processor board (MC-MP-xx or MC-PCA-xx). However, additional programming options are available via a CRT terminal or PC.

Using a CRT terminal or PC, up to eight Security Configurations can be programmed. The Security Configurations allow each floor to be designated as *unsecured*, *secured* or *locked* for car calls and either *unsecured* or *locked* for hall calls. These terms are defined as follows:

- unsecured = unrestricted access, all car and/or hall calls are registered
- secured = access restricted, valid security code required to register car calls
- locked = no access, car calls and/or hall calls are not registered

Floors for which a security code and a Security Configuration have been programmed are *secured* when that configuration is active and security is ON. In order to gain access to a secured floor via the elevator, the correct security code must be entered using the Car Operating Panel (COP) buttons. When the COP button for a secured floor is pressed, the button's indicator will flash to indicate that a security code is required. The passenger must enter the correct code within 10 seconds, otherwise the call will not be registered and the indicator will turn OFF.

Basic Security with CRT allows security to be turned ON or OFF and to determine which of eight Security Configurations is active on any day or time, based on a programmable time schedule called the Security Configuration Timer Table.

1.4 DESCRIPTION OF ACCESS CONTROL FOR ELEVATORS (ACE)

Access Control for Elevators (ACE) offers the most sophisticated programming capability. ACE provides a wide range of options allowing building owners and managers the greatest flexibility of any elevator security system.

ACE has passenger access codes which allow only authorized passengers access to building floors via the elevators. Each passenger or group of passengers can be assigned a unique access code. Each code can have its own unique set(s) of access permissions. The sets of access permissions can change based on date or day and time using one or more of six time schedules.

General Floor Access Control - Using a CRT terminal or PC, up to eight Security Configurations can be programmed. The Security Configurations allow each floor to be designated as *unsecured*, *secured* or *locked* for car calls and either *unsecured* or *locked* for hall calls. These terms are defined as follows:

- unsecured = unrestricted access, all car and/or hall calls are registered
- secured = access restricted, valid security code required to register car calls
- locked = no access, car calls and/or hall calls are not registered

ACE allows security to be turned ON or OFF and to determine which of eight Security Configurations is active on any date or day(s) and time, based on a programmable time schedule called the Security Configuration Timer Table.

Floors which have been designated as secured on a Security Configuration *are secured* when that configuration is active and security is ON. In order to gain access to a secured floor via the elevator, a Passenger Access Code (PAC) must be entered using the Car Operating Panel (COP) buttons. The PAC must have permission to access that floor on this day and time. When the COP button for a secured floor is pressed, the button's indicator will flash to indicate that a passenger access code is required. The passenger must enter the code within 10 seconds, otherwise the call will not be registered and the indicator will turn OFF.

PAC Access Control - Each Passenger Access Code (PAC) can have its own set of access permissions for each floor (access or no access). Each PAC has a Personal Time Schedule which can limit access to a specific date or day(s) and hours. In addition, each PAC can be included in one or more of four groups that have a Group Time Schedule which can limit access to a specific date or day(s) and hours.

Reports - While ACE Security is ON, each time an attempt is made to access a secured floor via the elevators, the date, time, floor, and passenger ID is logged. The 500 most recent attempts are saved and can be viewed and/or printed.

1.5 DESCRIPTION OF SECURITY INTERFACE SOFTWARE (SIS)

Security Interface Software (SIS) is used to program the elevator security parameters using a PC. Depending on the software type/version you have, SIS can be run on a PC:

- as a stand-alone DOS program
- launched from inside Windows
- as a native Windows application
- launched from MCE's Central Monitoring System (CMS) for Windows software.

The PC can be connected to the controller in the following ways:

- directly via serial cable
- via serial cable plus line drivers (to extend the distance)
- via a phone line using a modem.
- via an Ethernet connection.

1.6 AN OVERVIEW OF MCE'S ELEVATOR SECURITY

Normally when a passenger enters a hall call from a lobby or a car call from a car, the elevator will respond by taking the passengers wherever they want to go. With MCE's Basic Security with CRT or Access Control for Elevators (ACE) security, when the elevator system's Security Status is *ON*, the security status of each floor is defined by a Security Configuration and the elevator's response is determined by the security status of that floor.

A floor's security status for hall calls or car calls is determined by the currently active Security Configuration, called the *current configuration*. There are eight Security Configurations available but only one, the current configuration, is in use at any given time. A Security Configuration has one hall call map and a car call map for each car. You may manually choose the current configuration from among the eight Security Configurations, or program the Timer Table to automatically select the current configuration.

The security status for a ***hall call*** can be either ***Unsecured*** or ***Locked***. *Unsecured* for *hall calls* means that access to elevators from that floor is unrestricted. *Locked* for *hall calls* means that access to elevators from that floor is not permitted.

The security status for a ***car call*** can be ***Unsecured***, ***Locked*** or ***Secured***. *Unsecured* for *car calls* means that access to that floor is unrestricted. *Locked* for *car calls* means that access to that floor is not permitted. *Secured* for *car calls* means that access to that floor is permitted only if the proper security code or access code is entered via the car operating panel (COP) buttons.

With *Basic Security*, the Security Codes for each floor are programmed using the Car Controller's Main Computer. A floor can not be *Secured* unless a *Security Code* has been programmed. The Security Codes are viewed and changed using the individual Car Controller's Main Computer. More information about programming the Security Codes can be found in Section 2.3 titled *Viewing and Changing the Security Codes - PTC and PHC* or Section 2.4 titled *Setting the Security Codes - Swing Panel*.

With Access Control for Elevators (ACE), access codes, called Passenger Access Codes (PAC), are assigned to individual passengers or groups of passengers. Instructions for programming the ACE Passenger Access Codes are found in Section 5.7, *Assigning the Passenger Access Codes (PAC).*

The following is a description of what happens when hall calls are entered.

When a **hall** call button is pressed, the call **will be registered** if:

- Security is **OFF,** *or*
- Security is **ON** and this floor is **Unsecured**.

When a **hall** call button is pressed, the call **will *NOT* be registered** if:

- Security is **ON** and the floor is **Locked**.

The following is a description of what happens when car calls are entered.

When a **car** call button is pressed, the call **will be registered** if:

- Security is **OFF**, *or*
- Security is **ON** and the desired floor is **Unsecured**, *or*
- Security is **ON** and the desired floor is **Secured**, *and*
  - The Security Code for the floor or the PAC is entered within 10 seconds.

When a **car** call button is pressed, the call **will *NOT* be registered** if:

- Security is **ON** *and*,
  - the desired floor is **Locked**, *or*
  - the desired floor is **Secured**, and the Security Code or PAC is not entered within 10 seconds.

SECTION 2
BASIC SECURITY

2.0 GENERAL

This section pertains to MCE's Basic Security. Basic Security is implemented on each individual elevator car controller. Instructions for programming the Security Codes on both Computer Swing Panel and Programmable Controllers (PTC and PHC) are included.

2.1 DESCRIPTION

Basic Security provides a means to prevent registration of unauthorized car calls. Security codes can be assigned for each floor of a building. The security codes consist of one to eight landing labels and are programmed using the controller's Main Processor board (MC-MP-xx or MC-PCA-xx).

Floors for which a security code has been programmed are *secured* when Basic Security is turned ON. In order to gain access to a secured floor via the elevator, the correct security code must be entered using the Car Operating Panel (COP) buttons. When the COP button for a secured floor is pressed, the button's indicator will flash to indicate that a security code is required. The passenger must enter the correct code within 10 seconds, otherwise the call will not be registered and the indicator will turn OFF.

2.2 TURNING BASIC SECURITY ON AND OFF

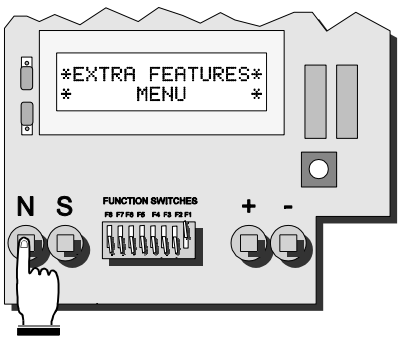
Basic Security is normally turned ON and OFF using the controller's Building Security Input (BSI). This input can be activated by a switch or external timer. On PTC and PHC controllers, Basic Security can also be turned ON and OFF using the controller's Master Software Key (MSK) setting.

MASTER SOFTWARE KEY (MSK) - PTC AND PHC

The Master Software Key is a board-level control of security. The Master Software Key can be set to ***Activated***, ***Deactivated*** or ***Enabled*** through the MC-PCA Main Computer board.

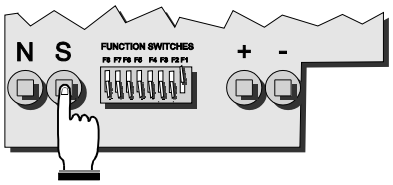
When the Master Software Key is set to *Activated*, Basic Security is ON. When the Master Software Key is set to *Deactivated*, Basic Security is OFF. When the Master Software Key is set to *Enabled*, Basic Security is turned ON and OFF via the Building Security Input (BSI).

CHANGING THE MASTER SOFTWARE KEY SETTING - Changes to the Master Software Key setting are made through the MC-PCA board's On-Board Diagnostics Menu.

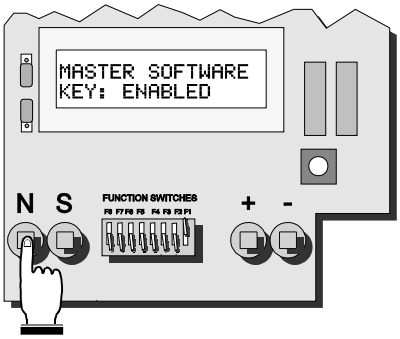


1. Place the car on Inspection.
2. Place function switch **F1** in the *Up* position.
3. Press the **N** push button until the *Extra Features Menu* appears on the display.

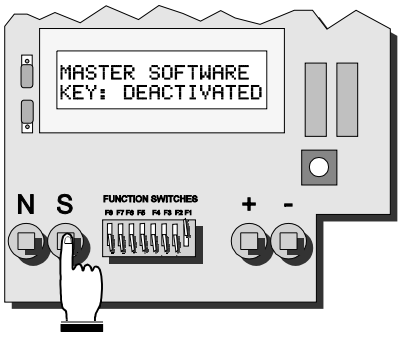
4. Press the **S** push button once.



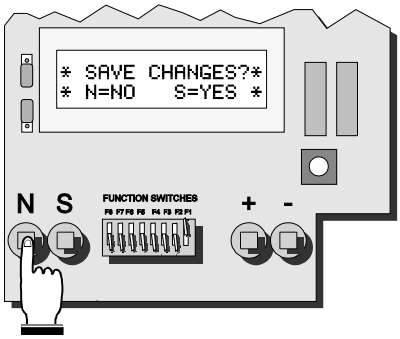
5. Then press the **N** push button until *Master Software Key:* appears on the display.



6. To change to current setting, press the **S** push button. The display will cycle through the available settings, *Activated, Deactivated* and *Enabled*. When the desired setting is displayed ...



7. Press the **N** push button until *Save Changes* is displayed. Press the **S** push button to *Save* the new Master Software Key setting and return the function switch **F1** to the *down* position.



CAUTION: Be careful not to inadvertently change other options on the controller, as any and all changes will be saved in the MC-PCA board as a result of the *Save Changes* operation. Section 5 of the controller manual describes, in detail, how to program the computer.

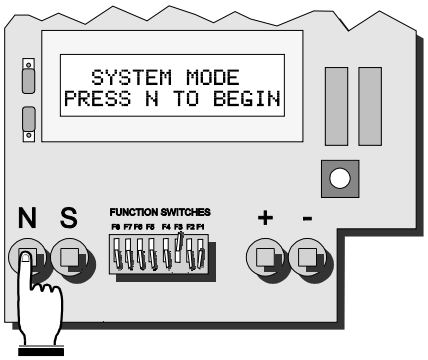
2.3 VIEWING AND CHANGING THE SECURITY CODES - PTC AND PHC

The Security code for each floor may consist of one to eight characters, each represented by one of the floor buttons found in the elevator car. **A floor can NOT be *Secured* unless a *Security Code* has been programmed.**

The Appendix titled ELEVATOR SECURITY INFORMATION AND OPERATION provides instructions for elevator passengers on the use of Security operation. Space has been provided for listing the security codes for each floor.

2.3.1 VIEWING THE BUILDING SECURITY MENU

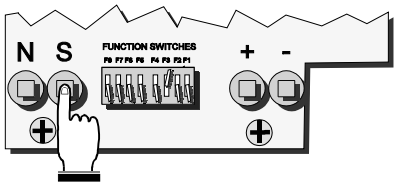
- On the MC-PCA Computer board, place the F3 switch in the up position (with all other switches in the down position). The following display appears:



- Press the N push-button.
- The following display will appear:

```
*     BUILDING     *
*  SECURITY MENU   *
```

2.3.2 PROGRAMMING THE SECURITY CODES

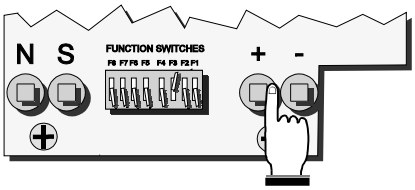


- Press the ***S*** push-button to start programming or changing the Security codes (or to view the codes).
- If no code has been programmed, the computer displays NO CODE PROGRAMMED for that particular floor number. Press the ***S*** push-button again to start programming the Security code.

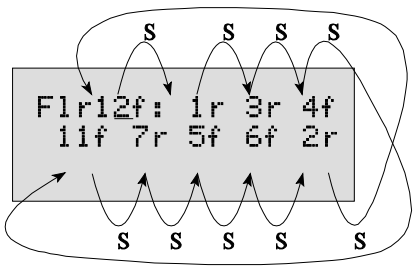
```
Flr 1f: NO
CODE PROGRAMMED
```

- If a code has already been programmed, the computer displays the security code. The cursor will blink below the floor number for the Security code being displayed.

```
Flr 1f: 8r 3f 4f
   2r21f31r19f17r
```



- Press the **+** and – push-buttons to select the floor number to change. The + push-button increments the floor being displayed to the next eligible floor. The – push-button decrements the value.
- Press the ***S*** pushbutton to move the cursor to the first character of the Security code. Press the **+** and – push-buttons to change the value of the first character. Repeat these steps (pressing the S push-button followed by the + and – pushbuttons) until the desired number of characters are programmed (maximum of 8 characters). The S push-button moves the position of the blinking cursor according to the diagram at the right. If any character is left blank, or after all eight characters are programmed, pressing the S pushbutton returns the cursor to the floor number.



- Repeat these steps to program the Security codes for all the floors. You may exit the Building Security Menu at any time during programming by pressing the ***N*** push-button. When the ***N*** push-button is pressed, the LCD will display the following:

```
Exit this menu?
  N=No S=Yes
```

- Press the ***S*** push-button to exit or the ***N*** push-button to return to the previous display. If ***S*** is pressed, the following will appear (only if changes have been made):

```
Save Changes?
  N=No S=Save
```

- Press ***S*** to save the changes or ***N*** to exit without saving (any original codes will remain in effect if the changes are not saved).

2.4 VIEWING AND CHANGING THE SECURITY CODES - SWING PANEL

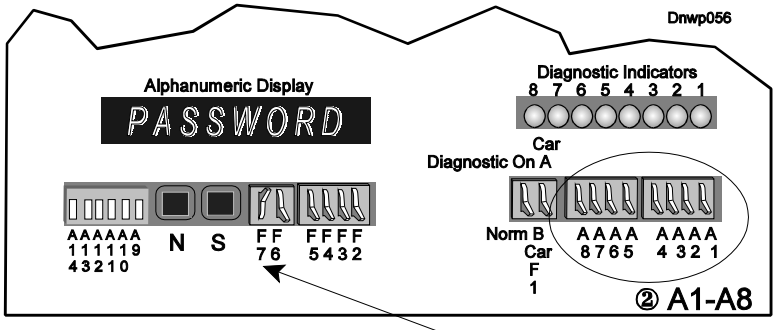
The security code for each floor may consist of from one to eight characters, where each character is one of the floor buttons found in the elevator car. Each floor may have a different length code. **A floor can not be *Secured* unless a *Security Code* has been programed.**

Appendix, *Security Information and Operation*, provides instructions for elevator passengers who will be using the elevator while Security is ON. Space has been provided for listing the security codes for each floor.

The Security Codes are viewed and changed using each ***Simplex or Local Car*** controller's Computer Swing Panel while in the "System Mode" of operation.

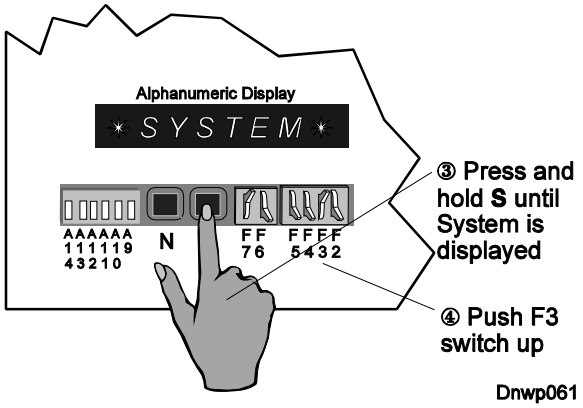
1. Place function switch ***F7*** in the *ON* (up) position. The alphanumeric display shows PASSWORD.

2. Set the A1 - A8 switches to the password value. If no password has been programmed for this job (which is normally the case), set A1 - A8 to OFF (down).



3. Press and hold the ***S*** push button until the alphanumeric display shows *SYSTEM*.The eight vertical status indicators scan from bottom to top. In System Mode, if function switches or pushbuttons are not pressed for two minutes, the computer exits System mode and returns to Normal mode.

4. Place the F3 switch to the *ON* (up) position. The display will show the 1st floor's security status. If "NOT USED" is displayed, the elevator is not equipped with the Security option.



5. To view subsequent floors security status, press the ***N*** pushbutton.

6. Table 2.1, *Changing the Floor Security Status and Security Code*, describes the steps required to change a floor's security code. Although it is possible to program each car to have a different Security Code for the same floor, this would be difficult to manage.

7. When viewing / changing is complete, move all switches to *OFF* (down) to exit System mode.

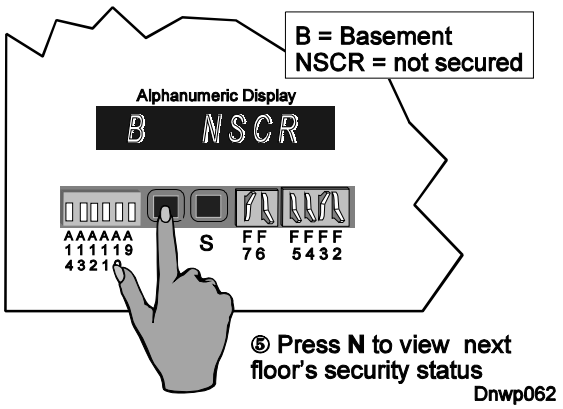


TABLE 2.1 Changing the Floor Security Status and Security Code (Simplex or Local Car)

Switch	Explanation	Alphanumeric Display
Step 1 **F3 ON (up)**	**To begin, display the 1st floor's status** While in the *System* mode, turn function switch F3 ON (up).	**Example:** ***B NSCR*** B = basement NSCR = not secured
Step 2 **Press N**	**To display another floor's security status** Steps to the next floor's security status. Press N again for the next floor, etc.	**Example:** ***1 SCRD*** 1 = floor #1 SCRD = secured
Step 3 **Press S**	**To select a floor to view or change a code** With the floor's security status displayed, press S. The first character of the floor's security code is then displayed.	**Example:** ***2 1=3*** For floor 2, the first character in the code is 3.
Step 4 **Press S**	**To change a code character** Steps through the available code characters. When the desired character is displayed, go to Step 5.	**Example :** ***2 1=5*** For floor 2, the first security character is now 5.
Step 5 **Press N**	**To display the next code character** Steps to the next character in the code. To change more characters, repeat steps 4 and 5. The last character of a code must be the word END if the code is less than eight characters long.	**Example 1:** ***2 2=4*** For floor 2, the second character in the code is 4. **Example 2:** ***2 1=END*** For floor 2, the first character in the security code is the word END. Floor 2 is unsecured.

Switch	Explanation	Alphanumeric Display
Step 6 **Press N**	**To end and save** If END is chosen as a code character or if this is the eighth character, when N is pressed the computer saves the code and displays the current floor's security status. To view or change the code for another floor, return to step 2.	**Example :** ***2 NSCR*** If END was chosen for first character, this floor has no security code and is unsecured. Using END for any other character just ends that code, but the floor is still secured.
F3 and F7 switches OFF (down)	**To exit System mode** Every security code must end with the word END or be 8 characters long. If not, the processor remains in System mode.	**Example:** ***11:04:27*** The time displayed

SECTION 3
BASIC SECURITY WITH CRT - SWING PANEL

3.0 GENERAL

This section pertains to Basic Security with CRT for Computer Swing Panel controllers. Refer to Section 4, *Basic Security with CRT - PTC and PHC* for PTC and PHC controllers. The screens depicted in this section are those found on an MCE controller using Release 4 Communication software. Some screens may look slightly different if your controller is running an earlier version of Communication software.

3.1 INTRODUCTION - PRODUCT DESCRIPTION

Basic Security with CRT is an extension of MCE's Basic Security. Basic Security with CRT is implemented in the Simplex / Local Car Controller and Group Supervisor in an M3 Group System. Programming is done mostly through a CRT terminal or PC, which can be connected to the controller directly or through a modem. The Master Software Key, however, is programmed using the Simplex or Group Controller's Computer Swing Panel and the Security Codes are programmed at each Simplex or Local Car Controller's Computer Swing Panel.

Basic Security with CRT features include:

- A flexible, easy to program, menu system.
- A user-programmable password regulates access to the menu system.
- There are eight programmable security configurations. The current Security Configuration can be manually selected via the CRT or it can be automatically selected by the Security Configuration Timer Table.
- There are sixteen programmable time schedules in the Security Configuration Timer Table. This gives the system the flexibility to automatically switch between the eight different Security Configurations.

Basic Security with CRT provides a means to prevent registration of unauthorized car calls and/or hall calls. As with Basic Security, the security codes for each floor are programmed using the controller's Main Processor board (MC-MP-xx or MC-PCA-xx). However, additional programming options are available via a CRT terminal or PC.

Using a CRT terminal or PC, up to eight Security Configurations can be programmed. The Security Configurations allow each floor to be designated as *unsecured*, *secured* or *locked* for car calls and either *unsecured* or *locked* for hall calls. These terms are defined as follows:

- unsecured = unrestricted access, all car and/or hall calls are registered
- secured = access restricted, valid security code required to register car calls
- locked = no access, car calls and/or hall calls are not registered

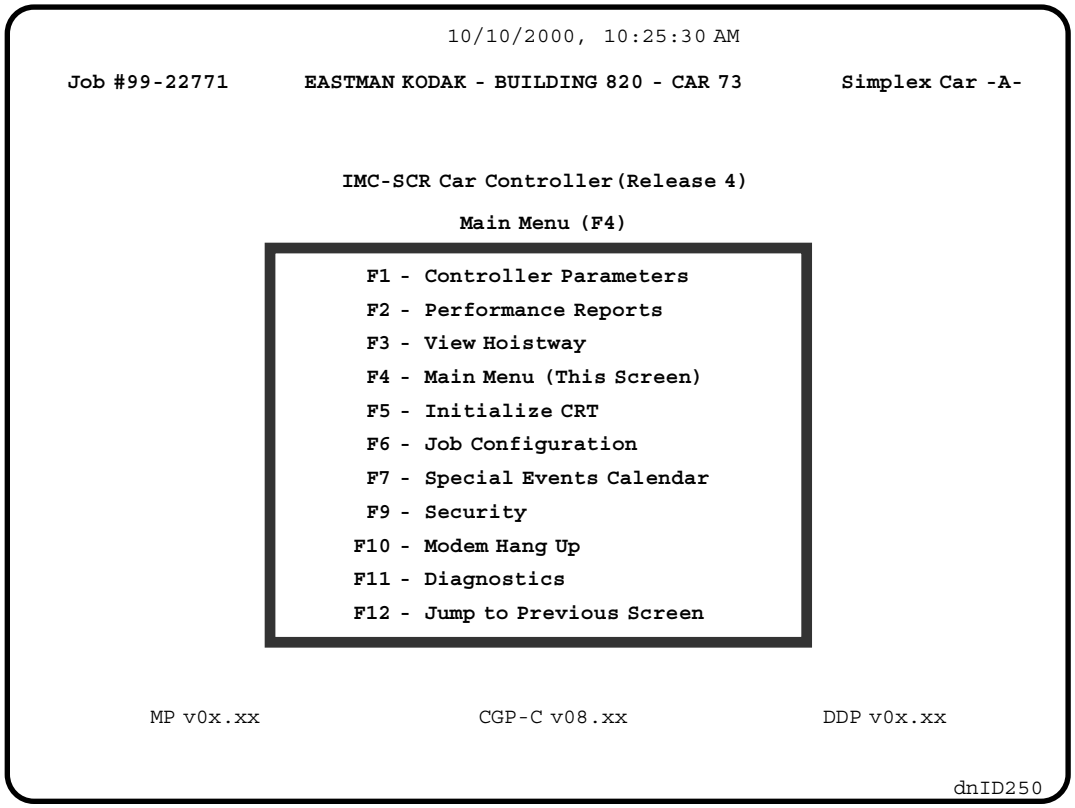
Floors for which a security code and a Security Configuration have been programmed are *secured* when that configuration is active and security is ON. In order to gain access to a secured floor via the elevator, the correct security code must be entered using the Car Operating Panel (COP) buttons. When the COP button for a secured floor is pressed, the button's indicator will flash to indicate that a security code is required. The passenger must enter the correct code within 10 seconds, otherwise the call will not be registered and the indicator will turn OFF.

Basic Security with CRT allows security to be turned ON or OFF, and to determine which of eight Security Configurations is active on any day or time, based on a programmable time schedule called the Security Configuration Timer Table.

3.1.1 MAIN MENU SCREEN

The **Main Menu** allows access to the Security Menu using selection F9, Security.

FIGURE 3.1 Main Menu



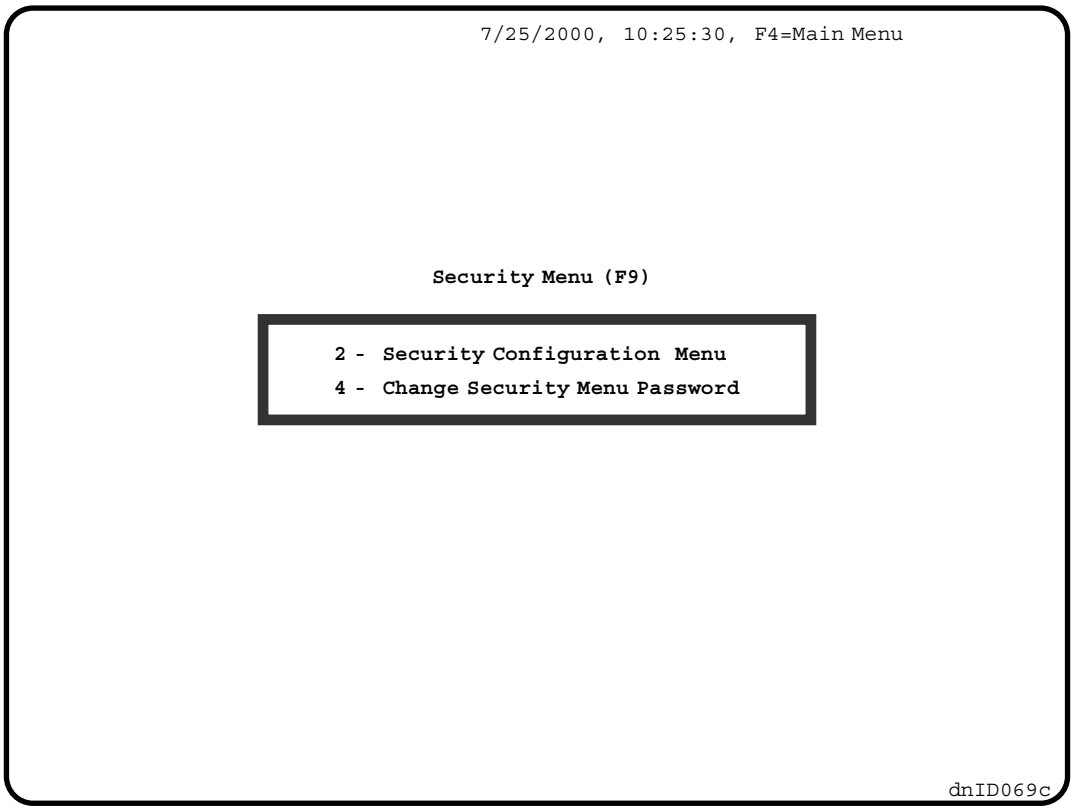
PASSWORD PROTECTED ACCESS TO THE SECURITY MENU - The Security Menu can be password protected. If no password is programmed, the Security Menu (Figure 3.2) will appear. If a password has been programmed, the following will appear when F9 is pressed:

Security Password: ■

Type in the password and press ENTER. The password itself will not appear on the screen. Instead, an asterisk (*) will appear for each character typed. When the correct password is entered the Security Menu will appear. Once a valid password has been entered, it is not necessary to re-enter the password unless you exit Security for more than ten minutes.

NOTE: The controller is shipped with no password programmed. Section 3.4 describes how to program or change the password.

FIGURE 3.2 Security Menu (F9) Screen



3.1.2 SECURITY MENU SCREEN

2 **Security Configuration Menu** - Select this menu if you would like to :

- program or modify a Security Configuration.
- program or modify the Security Configuration Timer Table.
- change the Current Security Configuration.
- change the Security Software Switch Status.

4 **Change Security Menu Password** - Use this to change the Password.

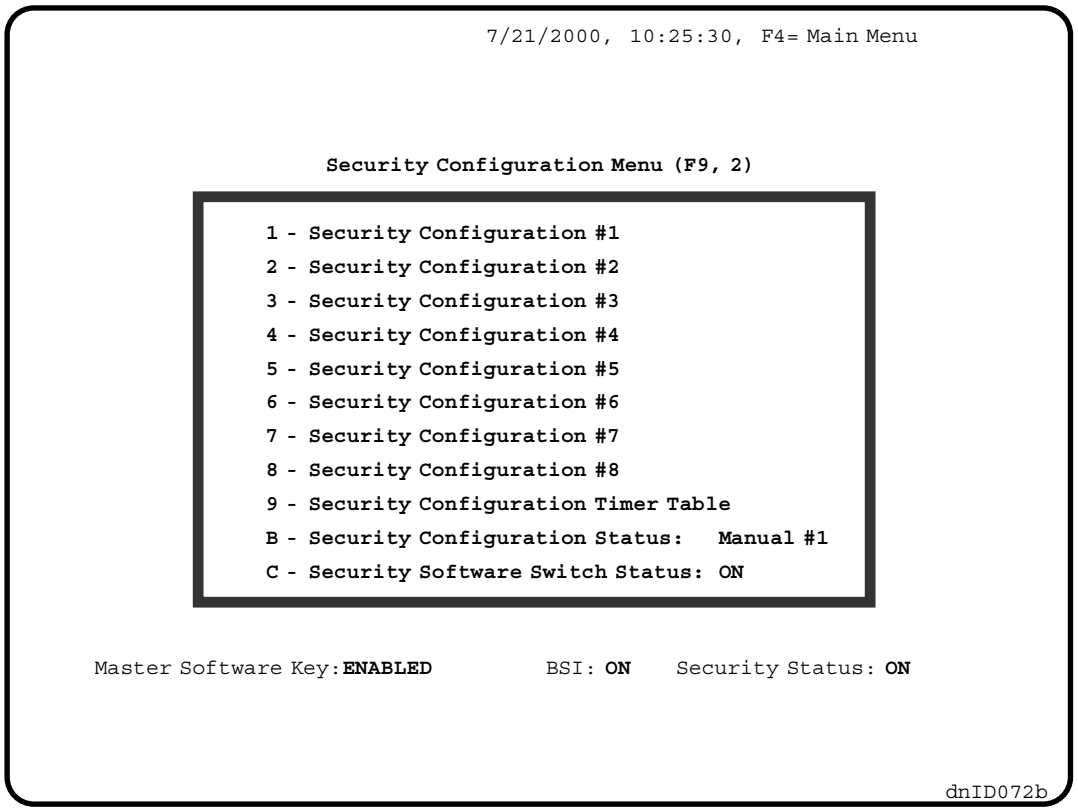
3.1.3 SECURITY CONFIGURATION MENU SCREEN

The Security Configuration Menu is accessed from the Security Menu by pressing 2. The following is a description of the items on Security Configuration Menu screen (Figure 3.3).

Security Configurations 1 thru 8 can be accessed by pressing 1 - 8. By programming a Security Configuration you can set the security status of each floor for Hall Calls (locked or unsecured) and for Car Calls (locked, unsecured or secured). Program one at a time. You don't have to program all eight of them. See Section 3.5 for programming details.

The **Security Configuration Timer Table**, selection 9, lets you set up a time schedule to determine which Security Configuration will be the *current configuration* when the Security Configuration Status is set to *Timed*. Each of sixteen timers can be programmed to select one of the eight Security Configurations. See Section 3.6 for details.

FIGURE 3.3 Security Configuration Menu (F9, 2) Screen



Security Configuration Status, selection B, allows manual selection of **Security Configuration #1 - #8** as *current configuration* , or **Timed** operation. The current status is displayed, i.e. Security Configuration Status: Manual #2, : Timed #3 or : Timed OFF. *Manual #2* means that Security Configuration #2 is the current configuration and it is manually selected. *Timed #3* means that Security Configuration #3 is the current configuration and it is selected via the Security Configuration Timer Table. *Timed OFF* means that Timed operation is selected and that System Security is *OFF* because none of the timers in the Security Configuration Timer Table are valid at this time. The Security Configuration Status option *Timed* will appear only if one of the sixteen timers in the Security Configuration Timer Table has a Timer Status of *On*.

Security Software Switch Status selection C, lets you set the Security Software Switch Status to *ON* or *OFF*. The current status is displayed, i.e. `Security Software Switch Status: ON`. The Security Software Switch Status is one of four elements that determine the System Security Status. The other three elements are the Master Software Key Status (see Section 3.2.1), the optional BSI Input (see Section 3.2.2) and the Security Configuration Status described above. The Security Status Decision Matrix (see Table 3.1) shows how each element affects the System Security Status.

Status Line - The line at the bottom of the screen is the status line. The status line contains important, continuously updated information on the status of the Master Software Key, BSI input, and System Security Status.

Security Status - The current status of the Elevator's Security system is displayed next to *Security Status.* It is determined by the status of the Master Software Key, BSI input, Security Software Switch, the Security Configuration Status, and the Security Configuration Timer Table if in *Timed* operation (see Section 3.2).

3.2 TURNING ELEVATOR SECURITY ON AND OFF

There are four elements that determine if Elevator Security is ON or OFF. These elements are:

- Master Software Key Status
- Security Software Switch Status
- BSI Input Status (optional)
- Security Configuration Status

The way in which each element affects the Security Status is depicted in the Security Status Decision Matrix, (Table 3.1).

TABLE 3.1 Security Status Decision Matrix

Inputs or Software Settings				Outputs or Results	
Master Software Key Status	**Security Software Switch Status**	**BSI✶ Input (optional)**	**Security Configuration Status**	**Security Configuration in use**	**Security Status**
Deactivated	n/a	n/a	n/a	none	**OFF**
Activated	n/a	n/a	n/a	1	**ON**
Enabled	ON	n/a	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table
	OFF	OFF	n/a	none	**OFF**
		ON	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table

✶ Ignore the shaded area unless the optional BSI input is included

3.2.1 MASTER SOFTWARE KEY STATUS

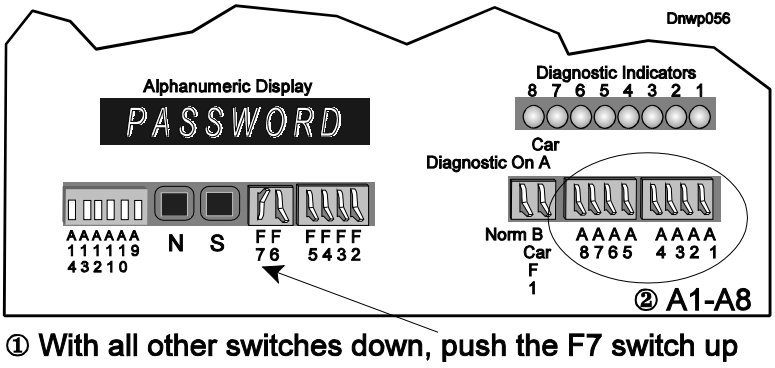
The Master Software Key is a board-level control of the security system mainly for use during periods when the CRT is not operational. The Master Software Key can be set to ***Activated***, ***Deactivated*** or ***Enabled*** through the controller's Computer Swing Panel.

When the Master Software Key is set to *Activated*, the Security Status is ON and Security Configuration #1 is in use. When the Master Software Key is set to *Deactivated*, the Security Status is OFF. When the Master Software Key is set to *Enabled*, the Security Status and the current configuration are determined by the status of the Security Software Switch, the BSI input (optional), and the Security Configuration Status (see Table 3.1, Security Status Decision Matrix).

CHANGING THE MASTER SOFTWARE KEY SETTING - Changes to the Master Software Key setting are made through the controller's Computer Swing Panel in *System Mode.*

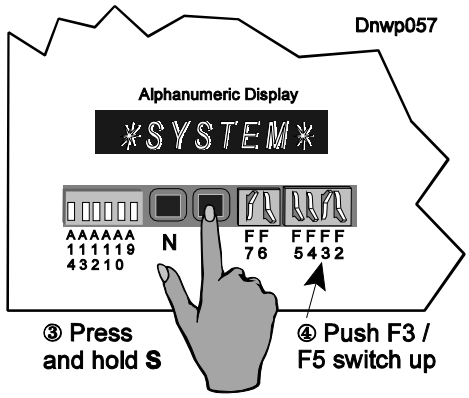
1. Place function switch ***F7*** in the *ON* (up) position. The alphanumeric display shows PASSWORD.

2. Set the A1 - A8 switches to the password value. If no password has been programmed for this job (which is normally the case), set A1 - A8 to OFF (down).



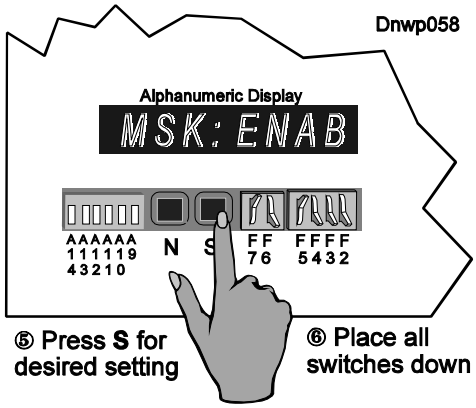
3. Press and hold the ***S*** push button until the alphanumeric display shows *SYSTEM*.The eight vertical status indicators scan from bottom to top. In System Mode, if function switches or pushbuttons are not pressed for two minutes, the computer exits System mode and returns to Normal mode.

4. Place function switch ***F3*** (*F5 on a Simplex Car)* in the *ON*, **up** position, to access the Master Software Key. The alphanumeric screen will display MSK: ENAB, MSK: ACTI, or MSK: DEAC. These are abbreviations for *Enabled*, *Activated*, or *Deactivated* respectively.



5. Press the **S** push button to change the current setting of the Master Software Key.

6. Place the **function switches** in the *OFF*, **down** position when finished. The normal state is *Enabled* so that Security can be controlled via the terminal.



3.2.2 SECURITY SOFTWARE SWITCH

When the Master Software Key is set to *Enabled*, changing the Security Software Switch Status can turn the building's security ON or OFF. Select [C] from the Security Configuration Menu to bring up the following selection line below the menu.

```
Set Security Software Switch: OFF  ON
```

Use [←] or [→] to move the cursor to **ON** or **OFF**, then press [ENTER].

The current status is continuously updated and displayed:

```
C - Security Software Switch Status: ON
```

3.2.3 BSI

The Building Security Input (BSI) is an input to the controller. It could be a connected to a hardware key-switch that is turned ON or OFF. The status of the BSI input is displayed next to it. Not all systems have the Building Security Input. If your system does not have this input, ignore BSI. Table 3.1 shows how the Security Status is affected by the BSI input.

3.2.4 SECURITY CONFIGURATION STATUS

The current Security Configuration can be selected manually or automatically (Timed). Manual selection means that the CRT terminal is used to manually select one of the eight Security Configurations to be the *current configuration*. Automatic selection means that the current configuration will be determined via the Security Configuration Timer Table. When the Security Configuration Status is *Timed*, the system will search the Security Configuration Timer Table constantly to achieve automatic selection of the *current configuration*. If none of the timers in the Security Configuration Timer Table is valid for the current day and time, then Security will be OFF. Security can be turned ON and OFF automatically via the Security Configuration Timer Table.

When one of the eight Security Configurations is selected manually, Security is ON if the Master Software Key is Enabled and the Security Software Switch and/or BSI is ON (see Table 3.1)

SETTING THE SECURITY CONFIGURATION MANUALLY - To manually select the Security Configuration press [B] in the Security Configuration Menu. The following line will appear under the Menu (the Timed option may not appear):

```
Select Current Configuration:  1  2  3  4  5  6  7  8  Timed
```

Use [←] or [→] to move the cursor or press [1] thru [8]. Select Security Configuration **1** thru **8** and press [ENTER]. The new status will then be displayed:

```
C - Security Configuration Status:  Manual #4
```

SETTING THE SECURITY CONFIGURATION AUTOMATICALLY (TIMED) - If you would like the system to automatically select different Security Configurations for different time periods based on the Security Configuration Timer Table, select [B] from the Security Configuration Menu. The following line will appear below the menu:(The *Timed* option will not be displayed unless at least one Timer in the Security Configuration Timer Table has a *Status* of ON).

```
Select Current Configuration:  1  2  3  4  5  6  7  8  Timed
```

Use [←] or [→] to move the cursor to **Timed** or press [T] and press [ENTER]. The new status will be displayed:

```
C - Security Configuration Status:  Timed #3
```

Timed #3 indicates that Timed mode of operation has been selected and Security Configuration #3 is the current configuration as determined by the Security Configuration Timer Table. If none of the timers in the Security Configuration Timer table are valid at this time (the current time falls between Start Time and End Time and Day includes today) the following will be displayed:

```
C - Security Configuration Status:  Timed OFF
```

3.3 USING THE CRT TERMINAL TO PROGRAM THE ELEVATOR SECURITY

The Elevator Security system must be properly programmed to set up the security for your building's needs. Here are some of the things that need to be programmed before running security on the elevator control system.

- Password for Security Menu access
- Security Configurations
- Security Configuration Timer Table

The following sections will explain how to program them. In this process you will use the following keys:

ENTER to make a selection or to confirm a selection.

ESC to abort or exit an operation, to exit a sub-menu.

1 to 9 to select a particular item from a Menu.

↑ ↓ ← → to move cursor around when programming or scrolling the screen.

TAB to quickly move the cursor from one field to another.

I and D to make changes. I to Increase a value. D to Decrease a value.

S to save the changes.

3.4 PROGRAMMING THE SECURITY MENU PASSWORD

Access to the Security Menu is password protected. The password may contain up to 8 characters. These characters may be alphabetic or numeric and can include spaces and punctuation. When no password is programmed you can access the Security Menu without restriction. There is no password programmed when the controller is shipped.

NOTE: You should program the password as soon as installation of the controller is completed.

3.4.1 CHANGING THE PASSWORD

To change or program the password, press 4 while the Security Menu is displayed (Figure 3.2). The screen will change to:

```
        Change Security Password (F9, 4)
Enter Current Password:
    Enter New Password:
  Confirm New Password:
```

Type in the current password and press ENTER. The password itself will not appear on the screen when you type it. Instead, an asterisk (*) will appear for each character typed.

Then type in the new password, up to eight characters, and press ENTER. The new password must be typed a second time for confirmation. The new password will not be displayed while being typed. An asterisk (*) will appear for each character typed.

3.4.2 LOST OR FORGOTTEN PASSWORD

If you lose or forget your password, type a question mark '?' at the password prompt and press ENTER. The following will appear on the screen:

```
MCE Security Reference #: XX
```

xx is a number between 0 to 15, randomly generated by the system.

Call MCE Technical Support and tell them the reference number. They will give you a temporary password. Type in the temporary password and press ENTER. If you make a mistake while typing the temporary password, try again. Then choose a new password, enter it and confirm it as described in Section 3.4.1.

3.5 PROGRAMMING THE SECURITY CONFIGURATIONS

A Security Configuration consists of a **Hall Call Map**, an **Auxiliary Hall Call Map** if an auxiliary hallway exists, and several **Car Call Maps**, one for each car (see Figure 3.4). The first column is the floor number displayed in landing labels, followed by columns for the Hall Call Map, Auxiliary Hall Call Map (not shown here), and Car Call Maps. The Auxiliary Hall Call Map will not be shown if the system is not equipped with auxiliary hall calls. The Car Label for each car is displayed on top of the Car Call Map.

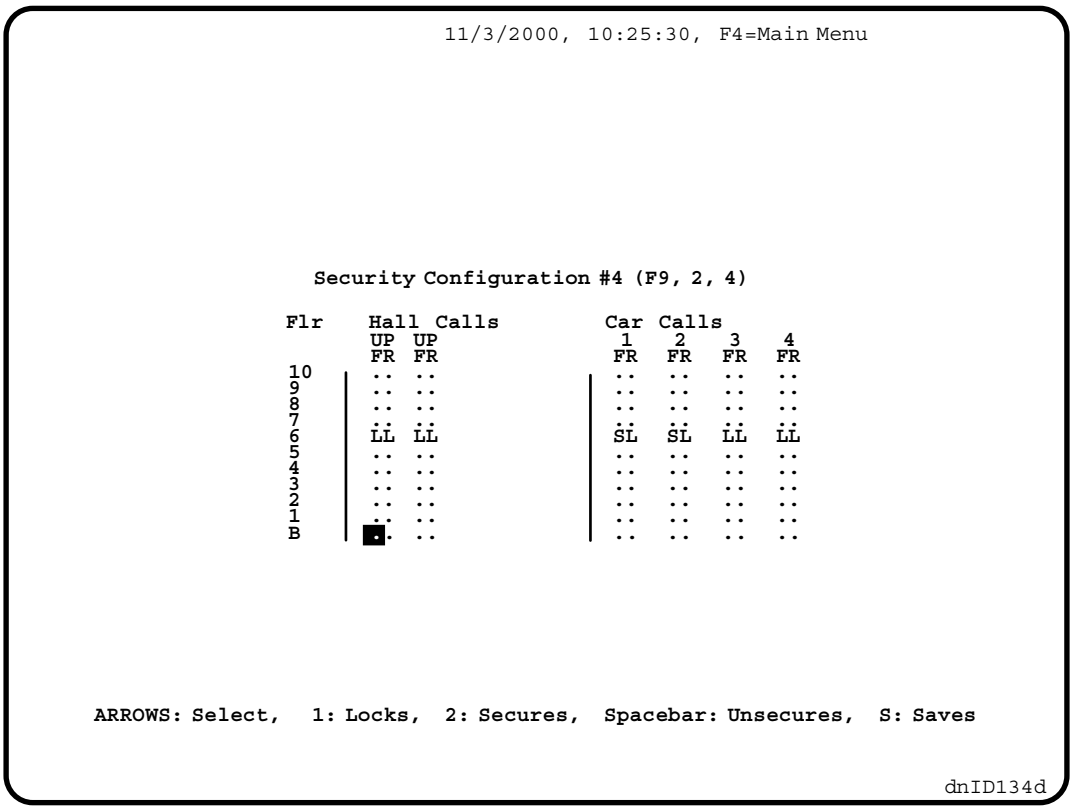
NOTE: Figure 3.5 shows an example of the optional Per-Car Hall and Car Call Mapping.

A floor's security status for ***hall calls*** can be either ***Unsecured*****,** indicated by a '**.**' or ***Locked*****,** indicated by an '**L**'. *Unsecured* for *hall calls* means that access to elevators from that floor is unrestricted. *Locked* for *hall calls* means that access to elevators from that floor is not permitted. The setting can be different for *Up* Hall Calls, column UP, and *Down* Hall Calls, column DN**,** on the same floor. Normally all floors, for hall calls, are unsecured so all hall calls are registered. When a floor is locked for hall calls, no one can leave that floor via the elevator.

A floor's security status for ***car calls*** can be ***Unsecured*****,** indicated by a '**.**', ***Locked*****,** indicated by an '**L**' or ***Secured*****,** indicated by an '**S**'. *Unsecured* for *car calls* means that access to that floor is unrestricted. *Locked* for *car calls* means that access to that floor is not permitted. *Secured* for *car calls* means that access to that floor is permitted only if the valid Security Code is entered within 10 seconds. **The security system can not *Secure* a floor unless a *Security Code* has been programmed as described in Section 3.7 *Viewing and Changing the Security Codes***.

If there are two different lobbies on the same floor, the floor's security status could be different for calls from different lobbies. The lobbies are symbolized by '**F**' and '**R**' indicating the ***Front*** door lobby and the ***Rear*** door lobby.

FIGURE 3.4 Security Configuration #4 (F9, 2, 4) Screen



PROGRAMMING THE HALL CALL AND CAR CALL MAPS - Use arrow keys to move the cursor and use I or D to change the floor security status. When I or D is pressed, the character under the cursor will switch between '**.**', '**L**' and '**S**'.

. = Unsecured — When a floor is Unsecured, all hall calls from the floor and car calls to the floor respond normally.

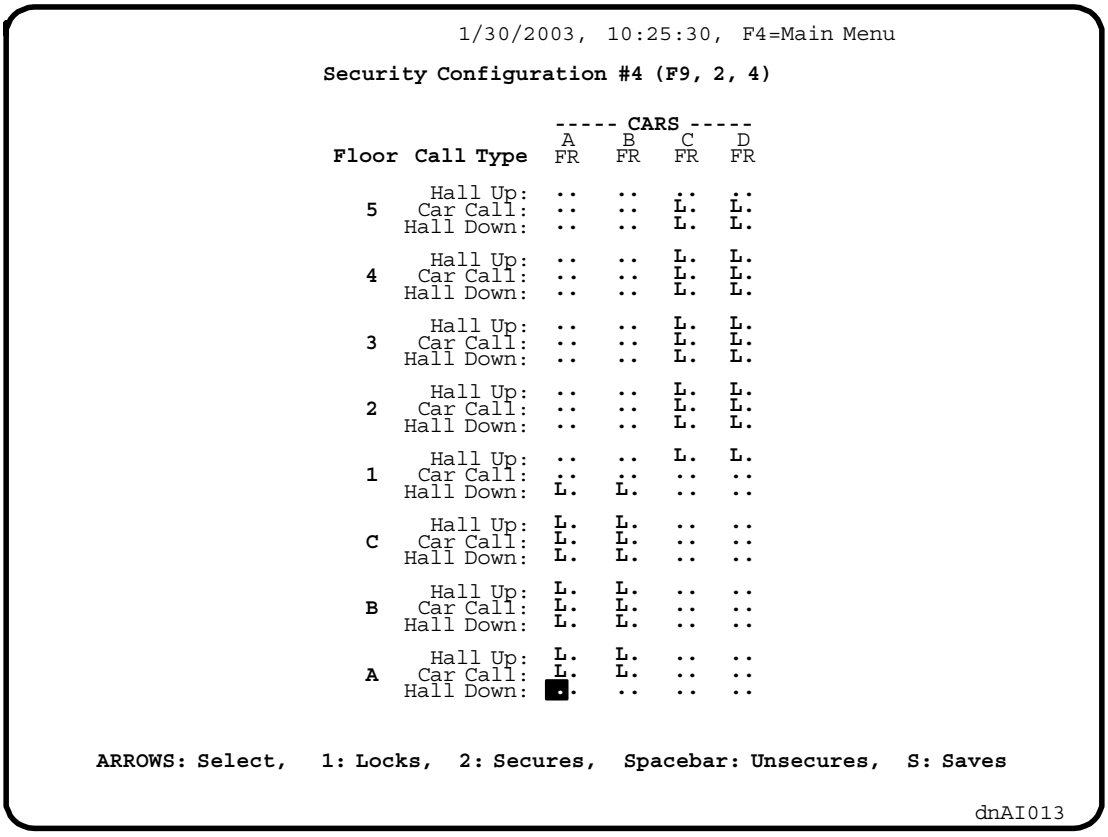
S = Secured — This status only exists for car calls. When a floor is Secured, access to the floor is restricted and any car call to that floor requires a valid Security Code.

L = Locked — When a floor is Locked, no hall calls or car calls are allowed to be registered. For a hall call, it means no one can leave the floor. For a car call, it means no one can go to that floor.

Use the **arrow keys** to move the cursor from one field to another and use the I and D keys to make changes. When you are ready to save the changes, press S. The system will ignore the S key if no entries were altered. Otherwise, a prompt **`Save changes? (Y/N)`** will appear at the bottom of the screen, press Y to confirm the save. Press N to not save the changes.

PER-CAR HALL AND CAR CALL MAPPING - If so ordered from the factory, your system may offer Per-Car Hall Call Security. Without Per-Car Hall Call Security, only car calls are configured on a per-car basis as shown in Figure 3.4. With Per-Car Hall Call Security, *both* hall and car calls may be configured on a per-car basis as shown in Figure 3.5.

FIGURE 3.5 Optional Per-Car Hall and Car Call Mapping



3.6 PROGRAMMING THE SECURITY CONFIGURATION TIMER TABLE

The Security Configuration Timer Table has 16 time schedules, Timer #1 thru #16. Each timer has a column for ***Start Date, End Date, Day***, ***Start Time***, ***End Time***, ***Action***, and ***Status***. The timers can be programmed to specify which Security Configuration will be the current configuration based on the date or day of the week, starting at Start Time and ending at End Time. The timer itself can also be set to *ON* or *OFF*, in use or not in use, via the Status.

When Master Software Key Status is *Enabled* and the BSI and/or the Security Software Switch Status is *ON*, and the Security Configuration Status is *Timed*, the controller will search the Security Configuration Timer Table for a timer with a Status of *ON*. The controller will then compare the current day and time with the day and time period defined in the timer. The highest priority timer found that has a defined day and time period into which the current day and time falls will be the active timer. The current configuration will be determined by the setting under ***Action*** in the active timer. The timers are searched continuously to achieve automatic switching of configurations.

NOTE: If no timers are found with a defined day and time period into which the current day and time falls, the Security Configuration Status will be **Timed OFF** and the Security Status will be **OFF**.

To program the Security Configuration Timer Table, press 9 at the Security Menu. The Security Configuration Timer Table screen will appear, as shown in Figure 3.6. All 16 timers (time schedules) are displayed and can be programmed on this screen. Each timer has seven programmable fields: ***Start Date, End Date, Day***, ***Start Time***, ***End Time***, ***Action***, and ***Status***. Timer #1 has highest priority and Timer # 16 has lowest priority. A timer's Status must first be changed to ON before other fields can be edited.

FIGURE 3.6 Security Configuration Timer Table (F9, 2, 9) Screen

12/11/2000, 10:25:30 AM, F4=Main Menu

Security Configuration Timer Table (F9,2, 9)

Priority High to Low	Start Date	End Date	Day	Start Time	End Time	Action	Status
Timer #1	7/4/2000	7/4/2000	DATE	07:00 AM	09:00 AM	Config #1	ON
Timer #2	--/--/--	--/--/--	M-F	11:00 AM	01:00 PM	Config #2	ON
Timer #3	--/--/--	--/--/--	MON	03:00 PM	06:00 PM	Config #3	ON
Timer #4	--/--/--	--/--/--	WED	03:OO PM	06:00 PM	Config #3	ON
Timer #5	--/--/--	--/--/--	FRI	03:00 PM	10:00 PM	Config #4	ON
Timer #6	12/25/2000	12/27/2000	DATE	07:00 AM	10:00 PM	Config #5	ON
Timer #7	--/--/--	--/--/--	---	--:--	--:--	-----	OFF
Timer #8	--/--/--	--/--/--	---	--:--	--:--	-----	OFF
Timer #9	--/--/--	--/--/--	---	--:--	--:--	-----	OFF
Timer #10	--/--/--	--/--/--	---	--:--	--:--	-----	OFF
Timer #11	--/--/--	--/--/--	---	--:--	--:--	-----	OFF
Timer #12	--/--/--	--/--/--	---	--:--	--:--	-----	OFF
Timer #13	--/--/--	--/--/--	---	--:--	--:--	-----	OFF
Timer #14	--/--/--	--/--/--	---	--:--	--:--	-----	OFF
Timer #15	--/--/--	--/--/--	---	--:--	--:--	-----	OFF
Timer #16	--/--/--	--/--/--	---	--:--	--:--	-----	OFF

Use the +/- keys to change the day on which this timer is active. Value may be a single day of the week like SAT for Saturday or a range of days M-F for Monday thru Friday. The setting ALL means the timer is active everyday. The setting DATE means the timer will be active only on the dates specified in the Date fields.

ARROWS: Select, +/-: Edits, S: Saves

dnID218b

EDITING METHODS - Use the **arrow keys** to select (highlight) the parameter to be edited. Instructions for editing appear at the bottom of the window. The method of editing varies depending on the selected field, i.e. when the Day, Action or Status fields are selected the **Space Bar** can be used to scroll through the available options or the **I** / **D** or **+** / **-** keys can be used to increment or decrement the value. To edit the Date field, the Day field must be set to DATE.

When the Start Time or End Time fields are selected, press **Enter** to edit and then type the new value. Most of the standard text editing keys are functional. Use the **Arrow** keys to select a character and type a new value over the old value. The **Insert** key toggles type-over and insert modes. The **Delete** key deletes the next character. The **Home** key moves the cursor to the far left and the **End** key moves the cursor to the far right. Press **Enter** when you have finished editing or **Esc** to cancel the edit.

SAVING THE CHANGES - Edited parameter values do not become effective until they are *saved*. Save the changes by pressing the **S** key. A message, **`Save changes? (Y/N),`** is displayed. Press **Y** to save or **N** to not save and continue editing. If you exit the screen without saving, the message, **`Save changes? (Y/N)`**, is displayed. Press **N** to exit without saving the changes. If **Y** is pressed, a confirmation message, **`Save Complete`**, is displayed. If there is a problem the message **`*** ERROR Saving Parameters ***`** is displayed. Contact MCE Technical Support for assistance.
The following is a description of the possible values for each field in the Security Configuration Timer Table:

Start Date and End Date - These fields specify the dates on which this timer will be active. To edit these fields, the Day field must be set to DATE.

Day - Day specifies the day or days of the week. There are ten choices: MON, TUE, WED, THU, FRI, SAT, SUN, M-F, ALL and DATE. M-F means Monday through Friday. ALL means all seven days of a week.

Start Time and End Time - These fields define the time period for each timer. The hour ranges from 0 to 23, and the minute ranges from 0 to 59. The earliest time is 12:00 AM (00:00) and the latest time is 12:00 AM (00:00). An End Time of 12:00 AM (00:00 means the timer stays active until the end of the day. Both start time and end time must be in the same day. No time period can be defined greater than 24 hours or defined across midnight.

Suppose you would like to use a configuration overnight. For example, suppose that Security Configuration #5 has been defined for 8:00 PM (20:00) to 6:00 AM (06:00) Monday through Friday. Use two timers and set the Day field of both timers to M-F. Set one timer's start time to 8:00 PM (20:00) and end time to 12:00 AM (00:00. Set the second timer's start time to 12:00 AM (00:00), and End Time to 6:00 AM (06:00). Set Action to Config #5 and Status *ON* for both timers.

CAUTION: Be careful not to define timers that overlap. If the *Start Time* of one timer is earlier than the *End Time* of another timer they may not operate as you expect.

Action - This field tells the system which Security Configuration to use in the time period defined by this timer.

Status - Status provides an easy way to turn a timer ON or OFF. If the Status is OFF, the Timer will not be used. If you set up a timer and for some reason you decide not to use it now, just turn the Status to OFF. Later when you want to use it again, set its status to ON.

Example : You would like the system to use Security Configuration #4 from 8 am to 4 pm, Monday through Friday.

Step 1: Program Security Configuration #4.

Step 2: Select [9] on the Security Configuration Menu.

Step 3: Find a free timer and set the **Status** to *ON.*

Step 4: Set the **Day** to M-F.

Step 5: Set the **Start Time** to 8:00 AM (08:00).

Step 7: Set the **End Time** to 4:00 PM (16:00).

Step 9: Set the **Action**, to Config #4.

Step 11: Press [S] then [Y] to save it.

Step 12: Press [ESC] to exit.

Repeat these steps to program other timers.

3.7 VIEWING AND CHANGING THE SECURITY CODES

The security code for each floor may consist of one to eight characters, where each character is one of the floor buttons found in the elevator car. Each floor may have a different code length. **A floor can not be *Secured* unless a *Security Code* has been programed.**

Appendix, *Security Information and Operation*, provides instructions for elevator passengers who will be using the elevator while Security is ON. Space has been provided for recording the security codes for each floor.

The Security Codes are viewed and changed using each ***Simplex or Local Car*** controller's Computer Swing Panel while in the "System Mode" of operation (see Section 3.2.1 for more information on System Mode).

1. Place the F7 switch in the *ON* (up) position. All other switches should be down.

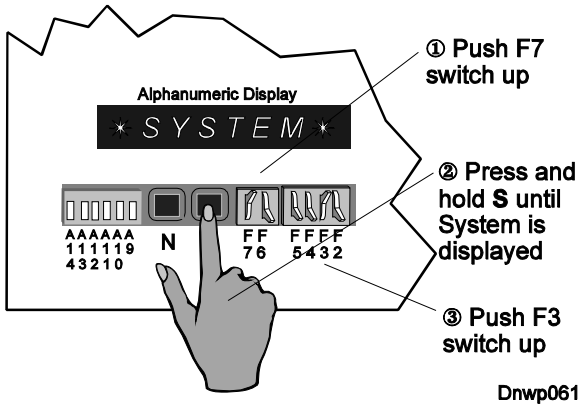
2. Press and hold the ***S*** pushbutton until **SYSTEM** appears in the alphanumeric display.

3. Place the F3 switch in the *ON* (up) position. The display will show the 1st floor's security status. If "NOT USED" is displayed, the elevator is not equipped with the Security option.

4. To view subsequent floor's security status, press the ***N*** pushbutton.

5. Table 3.2, *Changing the Floor Security Status and Security Code*, describes the steps required to change a floor's security code. Although it is possible to program each car to have a different Security Code for the same floor, this would be difficult to manage.

6. When viewing / changing is complete, move all switches to *OFF* (down) to exit System mode.



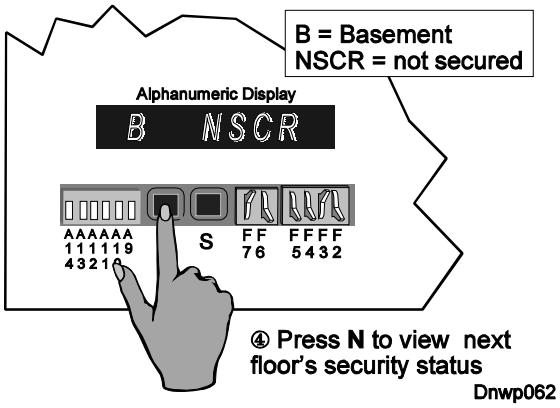


TABLE 3.2 Changing the Floor Security Status and Security Code (Simplex or Local Car)

Switch	Explanation	Alphanumeric Display
Step 1 **F3 ON (up)**	**To begin, display the 1st floor's status** While in the *System* mode, turn function switch F3 ON (up).	**Example:** `B NSCR` B = basement NSCR = not secured
Step 2 **Press N**	**To display another floor's security status** Steps to the next floor's security status. Press N again for the next floor, etc.	**Example:** `1 SCRD` 1 = floor #1 SCRD = secured
Step 3 **Press S**	**To select a floor to view or change a code** With the floor's security status displayed, press S. The first character of the floor's security code is then displayed.	**Example:** `2 1=3` For floor 2, the first character in the code is 3.
Step 4 **Press S**	**To change a code character** Steps through the available code characters. When the desired character is displayed, go to Step 5.	**Example :** `2 1=5` For floor 2, the first security character is now 5.
Step 5 **Press N**	**To display the next code character** Steps to the next character in the code. To change more characters, repeat steps 4 and 5. The last character of a code must be the word END if the code is less than eight characters long.	**Example 1:** `2 2=4` For floor 2, the second character in the code is 4. **Example 2:** `2 1=END` For floor 2, the first character in the security code is the word END. Floor 2 is unsecured.
Step 6 **Press N**	**To end and save** If END is chosen as a code character or if this is the eighth character, when N is pressed the computer saves the code and displays the current floor's security status. To view or change the code for another floor, return to step 2.	**Example :** `2 NSCR` If END was chosen for first character, this floor has no security code and is unsecured. Using END for any other character just ends that code, but the floor is still secured.
F3 and F7 switches OFF (down)	**To exit System mode** Every security code must end with the word END or be 8 characters long. If not, the processor remains in System mode.	**Example:** `11:04:27` The time displayed

3.8 PROGRAMMING CHECKLIST

Use following checklist to ensure that all of the elements required for proper operation of Basic Security with CRT have been programmed. Refer to the listed section for a description and instructions for programming each item.

1. Security Menu Password (Section 3.4).
2. Master Software Key (Section 3.2.1)
3. Security Software Switch (Section 3.2.2)
4. BSI Input, if applicable (Section 3.2.3)
5. Security Configuration Status (Section 3.2.4)
6. Security Configurations, as required (Section 3.5)
7. Security Configuration Timer Table (Section 3.6)
8. Security Codes (Section 3.7)

SECTION 4
BASIC SECURITY WITH CRT - PTC AND PHC

4.0 GENERAL

This section pertains to Basic Security with CRT for Programmable Traction Controllers (PTC) and Programmable Hydraulic Controllers (PHC). Refer to Section 3, *Basic Security with CRT - Swing Panel* for all other controllers.

4.1 INTRODUCTION - PRODUCT DESCRIPTION

Basic Security with CRT is an extension of MCE's Basic Security. The security configurations and timer table are programmed through a CRT terminal or PC connected to the MC-PA board. The Security Codes and Master Software Key are programmed at the controller's Main Processor (MC-PCA).

Basic Security with CRT features include:

- A flexible, easy to program, menu system.
- A user-programmable password for regulating access to the menu system.
- Eight programmable security configurations. The security configuration can be manually selected via the terminal or automatically selected by the Security Configuration Timer Table.
- Sixteen programmable time schedules in the Security Configuration Timer Table. This allows system flexibility to automatically switch between the eight different security configurations.

Basic Security with CRT provides a means to prevent registration of unauthorized car calls and/or hall calls. As with Basic Security, the security codes for each floor are programmed using the controller's Main Processor board (MC-PCA-xx). However, additional programming options are available via a CRT terminal or PC.

Using a CRT terminal or PC, up to eight Security Configurations can be programmed. The Security Configurations allow each floor to be designated as *unsecured*, *secured* or *locked* for car calls and either *unsecured* or *locked* for hall calls. These terms are defined as follows:

- unsecured = unrestricted access, all car and/or hall calls are registered
- secured = access restricted, valid security code required to register car calls
- locked = no access, car calls and/or hall calls are not registered

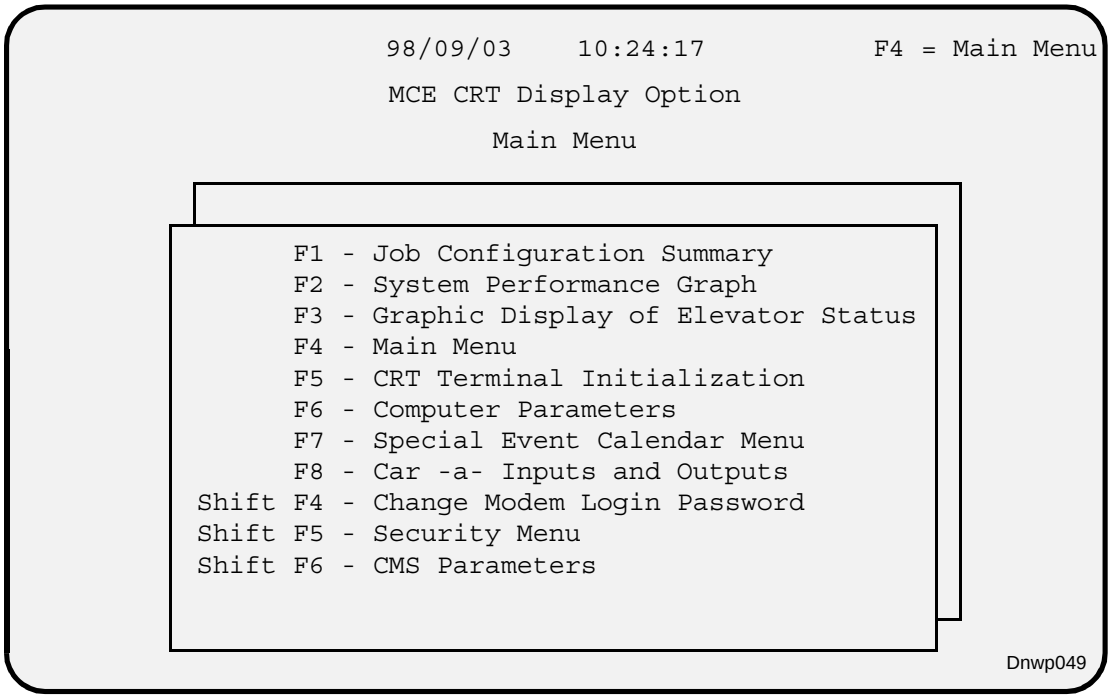
Floors for which a security code and a Security Configuration have been programmed are *secured* when that configuration is active and security is ON. In order to gain access to a secured floor via the elevator, the correct security code must be entered using the Car Operating Panel (COP) buttons. When the COP button for a secured floor is pressed, the button's indicator will flash to indicate that a security code is required. The passenger must enter the correct code within 10 seconds, otherwise the call will not be registered and the indicator will turn OFF.

Basic Security with CRT allows security to turned ON or OFF, and the determination as to which of the eight Security Configurations is to be active on any day or time, based on a programmable time schedule called the Security Configuration Timer Table.

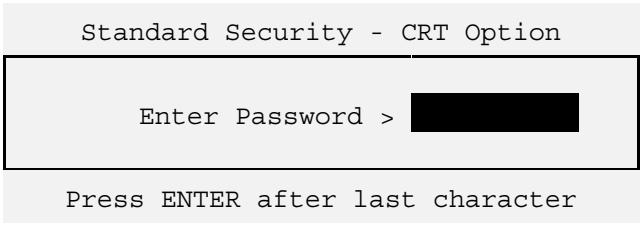
4.1.1 MAIN MENU SCREEN

The terminal's Main menu allows access to the Security Menu using selection SHIFT F5, Security Menu.

FIGURE 4.1 Main Menu



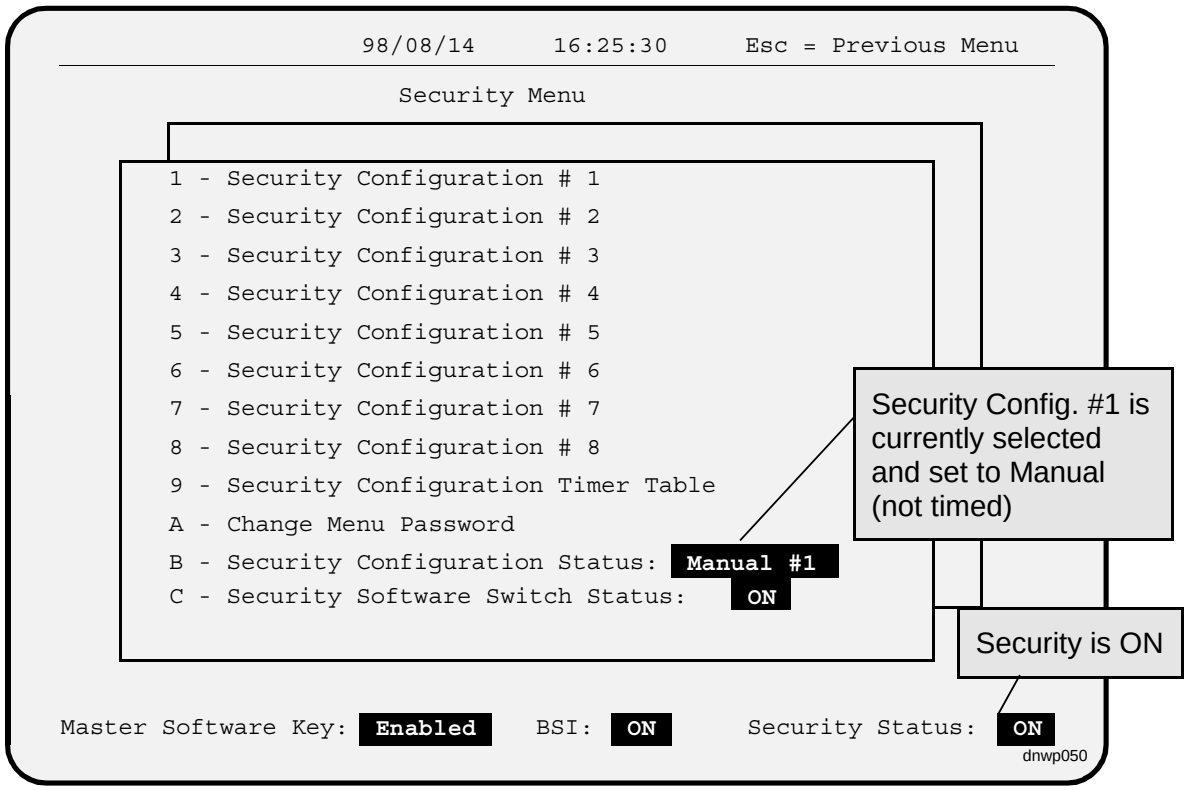
PASSWORD PROTECTED ACCESS TO THE SECURITY MENU - The Security Menu is a password protected screen. If no password is programmed, the Security Menu (Figure 4.2) will appear. If a password has been programmed, the following will appear.



Type in the password and press ENTER. The password itself will not appear on the screen. Instead, an asterisk (*) will appear for each character typed. When the correct password is entered, the Security Menu will appear.

NOTE: If no password has been programmed you can gain access to the Security Menu by pressing ENTER. The controller is shipped without a password programmed. Section 4.4 describes how to program or change the password.

FIGURE 4.2 Security Menu Screen



4.1.2 SECURITY MENU SCREEN

The following are descriptions of the items on the Security menu screen: (Figure 4.2).

Security Configurations 1 thru **8** are accessed by pressing 1 thru 8. By programming a Security Configuration you can set the security status of each floor for hall calls (locked or unsecured) and for Car Calls (locked, unsecured or secured). Program one floor at a time. Program only those needed. It is not necessary to program all eight. See Section 4.5 for details.

Security Configuration Timer Table, selection 9, is a time schedule for the Security Configurations. The table (schedule) determines when a security configuration will be *ON*, or the *current configuration*. The Security Configuration Status must be set to *Timed* for the timer table to have any effect. Each of sixteen timers can be programmed to select one of the eight Security Configurations. An asterisk (*) will appear next to the currently active timer. See Section 4.6 for details.

Change Menu Password, selection A, is used to set or change the Security Menu Password. Access to the Security Menu is restricted to users with a valid password. See Section 4.4.

Security Configuration Status, selection B is used to select **Security Configuration #1 - #8** as the *current configuration* manually, or set to **Timed** operation. The following are sample status messages and their meaning:

```
B - Security Configuration Status: Manual #4
```

Manual #4 = Security Configuration #4 is the current configuration and it is manually selected

```
B - Security Configuration Status: Timed #3
```

Timed # 3 = Security Configuration #3 is the current configuration and it is selected *via* the timer table

```
B - Security Configuration Status: Timed OFF
```

Timed OFF = Timed operation is selected, however the security status is OFF because none of the timers in the table are valid during this time.

Security Software Switch Status, selection C, lets you set the Security Software Switch Status to *ON* or *OFF*. The current status is displayed, for example:

```
B - Security Software Switch: ON
```

Status Line - The line at the bottom of the screen is the status line. The status line contains important, continuously updated, information on the status of the Master Software Key, BSI input and the Security Status (described below).

Security Status - The current status of the Elevator's Security system is displayed next to *Security Status.* It is determined by the status of the Master Software Key, BSI input, Security Software Switch, the Security Configuration Status, and the Security Configuration Timer Table if in *Timed* operation.

4.2 TURNING ELEVATOR SECURITY ON AND OFF

There are four elements that determine if Elevator Security is ON or OFF. These elements are:

- Master Software Key Status
- Security Software Switch Status
- BSI Input Status (optional)
- Security Configuration Status

The way in which each element affects the Security Status is depicted in the Security Status Decision Matrix Table 4.1.

Table 4.1 Security Status Decision Matrix

Inputs or Software Settings				Outputs or Results	
Master Software Key Status	**Security Software Switch Status**	**BSI✶ Input (optional)**	**Security Configuration Status**	**Security Configuration in use**	**Security Status**
Deactivated	n/a	n/a	n/a	none	**OFF**
Activated	n/a	n/a	n/a	1	**ON**
Enabled	ON	n/a	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table
	OFF	OFF	n/a	none	**OFF**
		ON	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table

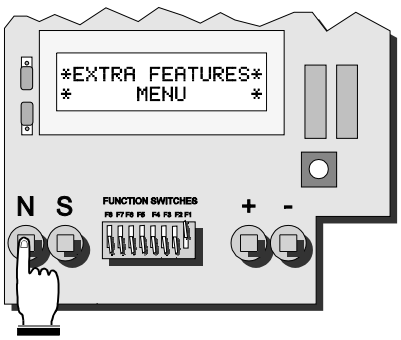
✶ Ignore the shaded area unless you have a BSI input to the controller.

4.2.1 MASTER SOFTWARE KEY STATUS

The Master Software Key is a board-level control of the security system mainly for use during periods when the CRT terminal or PC is not operational. The Master Software Key can be set to ***Activated***, ***Deactivated*** or ***Enabled*** through the MC-PCA Main Computer board.

When the Master Software Key is set to *Activated*, the Security Status is *On* and Security Configuration #1 is in use. When the Master Software Key is set to *Deactivated*, the Security Status is *Off*. When the Master Software Key is set to *Enabled*, the Security Status and the current configuration are determined by the status of the optional BSI input the Security Software Switch and the Security Configuration Status (see Table 4.1, Security Status Decision Matrix).

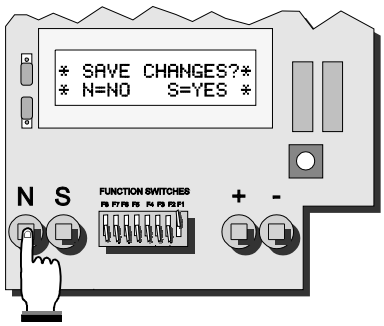
CHANGING THE MASTER SOFTWARE KEY SETTING - Changes to the Master Software Key setting are made through the MC-PCA board's On-Board Diagnostics Menu.



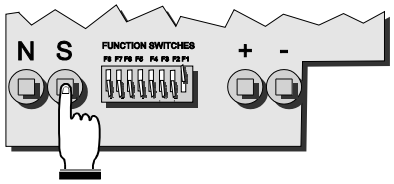
1. Place the car on Inspection.

2. Place function switch **F1** in the *Up* position.

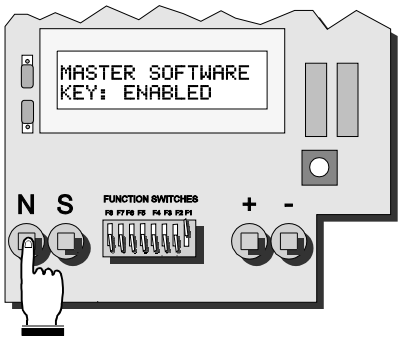
3. Press the **N** push button until the *Extra Features Menu* appears on the display.



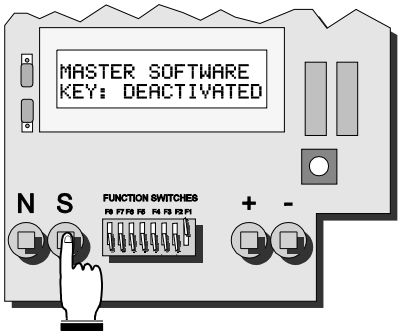
4. Press the **S** push button once.



5. Then press the **N** push button until *Master Software Key:* appears on the display.



6. To change to current setting, press the **S** push button. The display will cycle through the available settings, *Activated, Deactivated* and *Enabled*. When the desired setting is displayed ...



7. Press the **N** push button until *Save Changes* is displayed. Press the **S** push button to *Save* the new Master Software Key setting and return the function switch **F1** to the *down* position.

CAUTION: Be careful not to inadvertently change other options on the controller, as any and all changes will be saved in the MC-PCA board as a result of the *Save Changes* operation. Section 5 of the controller manual describes, in detail, how to program the computer.

4.2.2 SECURITY SOFTWARE SWITCH

When the Master Software Key is set to Enable, changing the Security Software Switch Status can toggle the building's Security Status ON or OFF. Select [C] from the Security Menu to bring up the following selection line below the menu.

```
Select Security Software Switch >   OFF  ON
```

Use [←] or [→] to move the cursor to **ON** or **OFF**, then press [ENTER].

The current status is continuously updated and displayed:

```
C - Security Software Switch Status:  OFF  ON
```

4.2.3 BSI

The Building Security Input (BSI) is an input to the controller. It could be connected to a hardware key-switch that is turned on or off. The current status of the BSI input is displayed on the Security Menu Status Line. Not all systems require the Building Security Input. If your system does not have this input, ignore BSI. Table 4.1 shows how the Security Status is affected by the BSI input.

4.2.4 SECURITY CONFIGURATION STATUS

The current Security Configuration can be selected manually or automatically (Timed). Manual selection means that you manually select *one* of the eight Security Configurations to be the *current configuration*. Automatic selection means that the current configuration will be determined by the Security Configuration Timer Table. When the Security Configuration Status is *Timed*, the system will search the Security Configuration Timer Table constantly to achieve automatic selection of the *current configuration*. If none of the timers in the Security Configuration Timer Table are valid for the current day and time, then the Security Status will be OFF.

When one of the eight Security Configurations is selected manually, the Security Status is ON if the Master Software Key is Enabled and the Security Software Switch and/or BSI are ON (see Table 4.1)

SETTING THE SECURITY CONFIGURATION MANUALLY - To manually select the Security Configuration press [B] in the Security Menu. The following line will appear under the Menu (the Timed option may not appear):

```
Select Security Configuration >  1 2 3 4 5 6 7 8 Timed
```

Use [←] or [→] to move the cursor or press [1] thru [8]. Select Security Configuration **1** thru **8** and press [ENTER]. The new status will then be displayed:

```
B – Security Configuration Status: Manual #4
```

SETTING THE SECURITY CONFIGURATION AUTOMATICALLY (TIMED) - To set the system to automatically select different security configurations for different time periods based on the Security Configuration Timer Table , select B from the Security menu (the *Timed* option will not display unless at least one timer in the Security Configuration Timer Table has a status of *ON*). After pressing B the following line will appear below the menu:

```
Select Security Configuration >  1 2 3 4 5 6 7 8 Timed
```

Use ← or → to move the cursor to **Timed** or press T and press ENTER. The new status will be displayed:

```
B – Security Configuration Status: Timed #3
```

Timed #3 indicates that Timed mode of operation is selected and Security Configuration #3 is the current configuration as determined by the Timer Table. If none of the timers in the Security Configuration Timer table are valid (the current time falls between start time and end time and day selected) the following will be displayed:

```
B – Security Configuration Status: Timed OFF
```

4.3 USING THE CRT TERMINAL TO PROGRAM THE ELEVATOR SECURITY

The Elevator Security system must be properly programmed for your building's needs. Three things that need to be programmed before running security on the elevator control system are as follows:

- ☞ **Password for Security Menu access**
- ☞ **Security Configurations**
- ☞ **Security Configuration Timer Table**

The following sections will explain how to program the security system. Table 4.2 describes the keystrokes used in programming the system.

TABLE 4.2 Programming Keystrokes

ENTER	to make a selection or to confirm a selection.
ESC or F12	to abort or exit an operation, to exit a sub-menu.
F1 to F10	to select a particular item from a Menu.
SHIFT	used together with a function key to make a selection.
PG↑ PG↓	to quickly scroll when programming or when viewing the diagnostic records.
↑ ↓ ← →	to move cursor around when programming or scrolling the screen.
TAB	to quickly move the cursor from one field to another.
I and D	to make changes. I to Increase a value. D to Decrease a value.
S or ALT S	to save the changes.

4.4 PROGRAMMING THE SECURITY MENU PASSWORD

Access to the Security Menu is password protected. The password may contain up to 8 characters. These characters may be alphanumeric and can include spaces and punctuation. When no password is programmed, you can access the Security Menu by pressing ENTER. There is no password programmed when the controller is shipped.

NOTE: You should program the password as soon as installation of the controller is completed.

4.4.1 CHANGING THE PASSWORD

To change the program password, press A while the Security menu is displayed. The screen will change to:

```
Modify Security Menu Password

Enter Current Password > ________

Press ENTER after last character
```

Type in the current password and press ENTER. If a password has not been programmed simply press ENTER. The password itself will not appear on the screen when entered. Instead, an asterisk (*) will appear for each character typed. The screen then changes to:

```
Modify Security Menu Password

Type New Password > ________

Press ENTER after last character
```

Type in the new password, up to eight characters, and press ENTER. The screen changes to:

```
Modify Security Menu Password

Retype New Password > ________

Press ENTER after last character
```

The new password must be typed a second time for confirmation. The new password does not display while being typed. An asterisk (*) will appear for each character typed.

4.4.2 LOST OR FORGOTTEN PASSWORD

If the password is lost or forgotten, type **?** (a question mark) where the password is entered. The following will appear on the screen:

MCE Security Reference #: xx

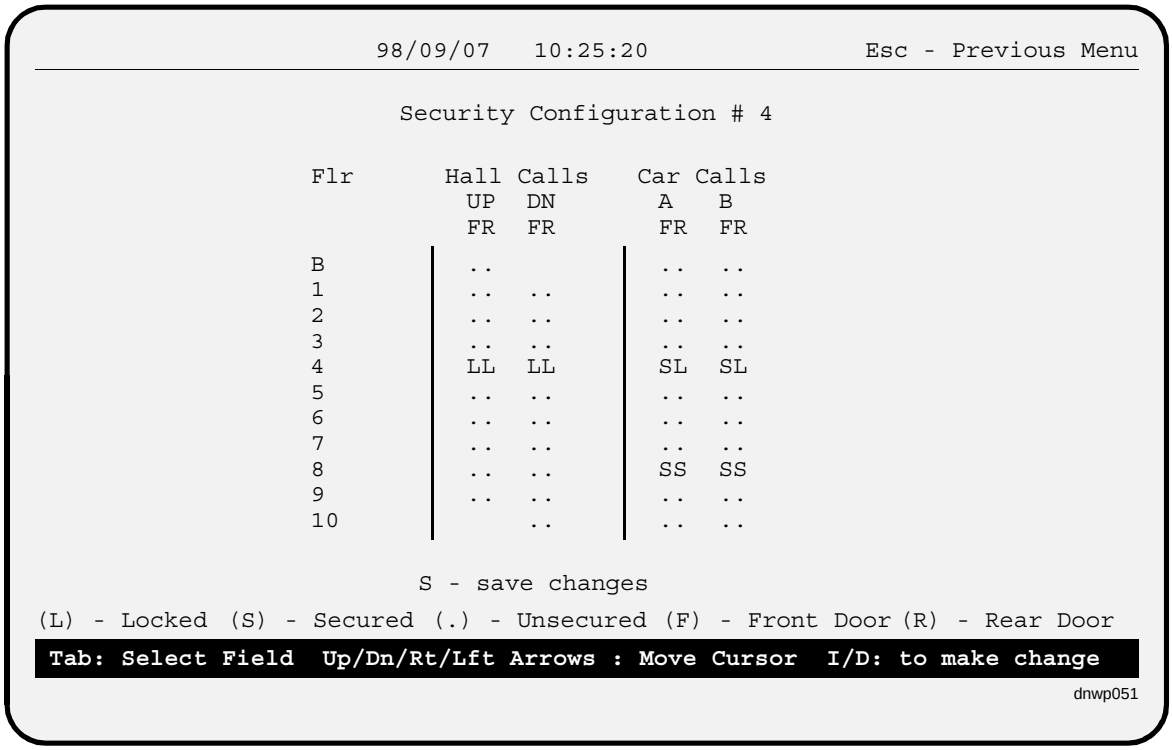
xx is a number between 0 to 15, randomly generated by the system.

Call MCE Technical Support and tell them the reference number. They will give you a temporary password. Type in the temporary password and press ENTER. If you make a mistake while typing the temporary password, try again. Then choose a new password, enter it and confirm it as described in Section 4.4.1.

4.5 PROGRAMMING THE SECURITY CONFIGURATIONS

A Security Configuration consists of a **Hall Call Map** and a **Car Call Map** for each car (see Figure 4.3). The first column is the floor landing label, followed by columns for the Hall Call and Car Call Maps. The Car Label for each car is displayed at the top of each Car Call Map column. If there are two different lobbies on the same floor, the floor's security status can be different for each call. The lobbies are symbolized as **F** for front door lobby and **R** for rear door lobby.

FIGURE 4.3 Security Configuration Screen



PROGRAMMING THE HALL CALL AND CAR CALL MAPS - Use the arrow keys to move the cursor, and use I or D to change the floor security status. When I or D is pressed, the character under the cursor will switch between **(.)**, **(L)** and **(S)**.

(.) Unsecured — When a floor is Unsecured, all hall calls from the floor and car calls to the floor respond normally.

(S) Secured — This status exists only for car calls. When a floor is Secured, access to the floor is restricted and any car call to that floor requires a valid Security Code.

(L) Locked — The hall and car calls are programmed, as locked, separately in individual columns. When a floor is Locked for hall calls, no hall calls are allowed to be registered. When a floor is Locked for car calls, no car calls are allowed to be registered.

To save the changes, press S. The system will ignore the S key if no entries were altered. Otherwise, a prompt **Are you sure? (y/n)** will blink at the bottom of the screen. Press Y to confirm the save or press any other key and the system will abandon the save.

4.6 PROGRAMMING THE SECURITY CONFIGURATION TIMER TABLE

The Security Configuration Timer Table has 16 time schedules, Timer #1 thru #16. Each timer has a column for ***Day***, ***Start Time***, ***End Time***, ***Config. #***, and ***Timer Status***. The timers can be programmed to specify which Security Configuration will be the current configuration based on the day of the week, start time and end time. The timer itself can also be set to *ON* or *OFF*, in use or not in use, by the Timer Status.

When Master Software Key Status is *Enabled* and the BSI and/or the Security Software Switch Status is *ON*, and the Security Configuration Status is *Timed*, the controller will search the Security Configuration Timer Table for a timer with a Timer Status of *ON*. The controller will then compare the current day and time with the day and time period defined in the timer. The highest priority timer found that has a defined day and time period into which the current day and time falls will be the current timer. Timer priority is determined by the timer number and the setting in the Day field. Timer #1 has highest priority and Timer # 16 has lowest priority, however, a timer with a Day field setting of a day of the week, **MON**, has a higher priority than a setting of **M-F**, which has a higher priority than a setting of **ALL**. The current configuration will be determined by the setting under ***Config #*** in the current timer. The timers are searched continuously to achieve automatic switching of configurations.

NOTE: If no timers are found with a defined day and time period into which the current day and time falls, the Security Configuration Status will be **Timed OFF** and the system's Security Status will be **OFF**.

4.6.1 PROGRAMMING INSTRUCTIONS

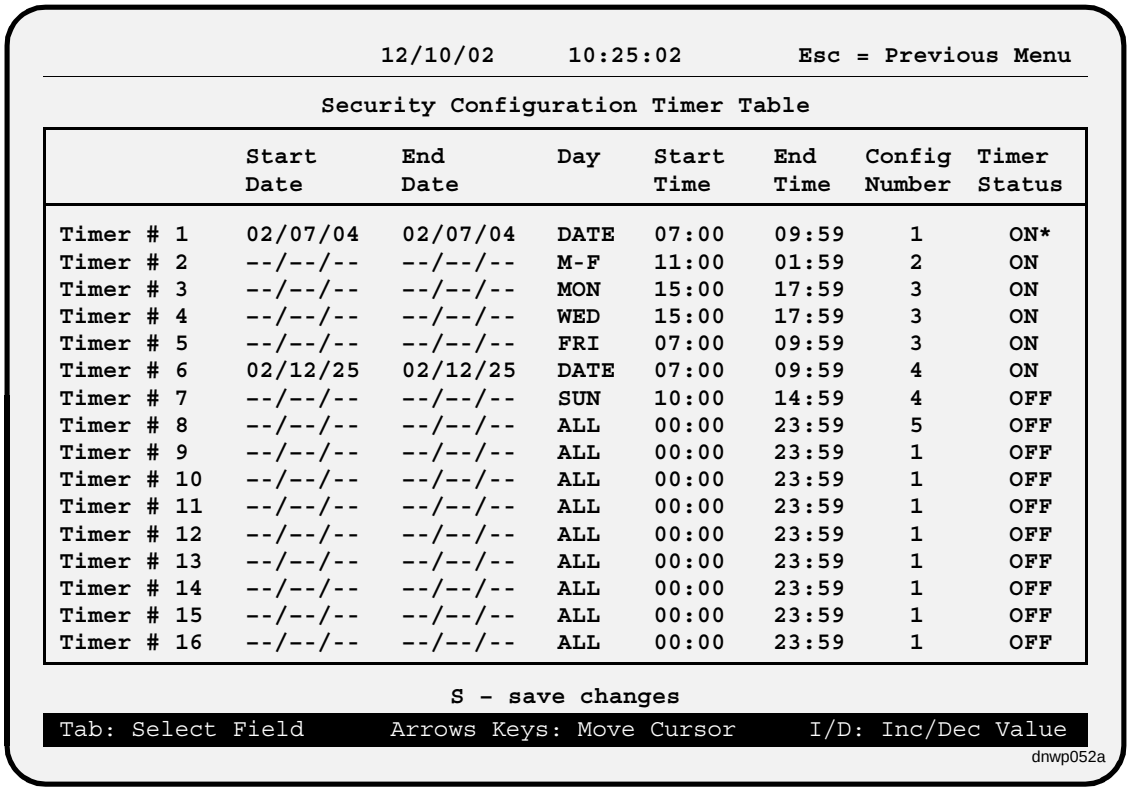
To program the Security Configuration Timer Table, press the: [9] key in the Security Menu. The Security Configuration Timer Table screen will appear, as shown in Figure 4.4. All 16 timers (time schedules) are displayed and can be programmed on this screen. Each timer has seven programmable fields: ***Day***, ***Start hour***, ***Start minute***, ***End hour***, ***End minute***, ***Config.*** #, and ***Timer Status***.

Use the **arrow keys** or the [TAB] key to move the cursor from one field to another and use the [I] and [D] keys to make changes.

To save the changes, press [S]. If changes were made, the system will prompt: **Are you sure? (y/n)**. Press [Y] to confirm the save or press any other key and the system will abandon the save.

Press the [ESC] key to exit. If changes were made without saving, the system will prompt: **Abandon Changes? (y/n)**. Press [Y] to abandon changes and exit or press any other key to automatically save the changes.

FIGURE 4.4 Security Configuration Timer Table



12/10/02 10:25:02 Esc = Previous Menu

Security Configuration Timer Table

	Start Date	End Date	Day	Start Time	End Time	Config Number	Timer Status
Timer # 1	02/07/04	02/07/04	DATE	07:00	09:59	1	ON*
Timer # 2	--/--/--	--/--/--	M-F	11:00	01:59	2	ON
Timer # 3	--/--/--	--/--/--	MON	15:00	17:59	3	ON
Timer # 4	--/--/--	--/--/--	WED	15:00	17:59	3	ON
Timer # 5	--/--/--	--/--/--	FRI	07:00	09:59	3	ON
Timer # 6	02/12/25	02/12/25	DATE	07:00	09:59	4	ON
Timer # 7	--/--/--	--/--/--	SUN	10:00	14:59	4	OFF
Timer # 8	--/--/--	--/--/--	ALL	00:00	23:59	5	OFF
Timer # 9	--/--/--	--/--/--	ALL	00:00	23:59	1	OFF
Timer # 10	--/--/--	--/--/--	ALL	00:00	23:59	1	OFF
Timer # 11	--/--/--	--/--/--	ALL	00:00	23:59	1	OFF
Timer # 12	--/--/--	--/--/--	ALL	00:00	23:59	1	OFF
Timer # 13	--/--/--	--/--/--	ALL	00:00	23:59	1	OFF
Timer # 14	--/--/--	--/--/--	ALL	00:00	23:59	1	OFF
Timer # 15	--/--/--	--/--/--	ALL	00:00	23:59	1	OFF
Timer # 16	--/--/--	--/--/--	ALL	00:00	23:59	1	OFF

S - save changes

Tab: Select Field Arrows Keys: Move Cursor I/D: Inc/Dec Value

dnwp052a

All Security Configuration Timer Table entry fields are described following:

Start Date and End Date - These fields specify the dates on which this timer will be active. To edit these fields, the Day field must be set to DATE.

Day - There are ten choices: MON, TUE, WED, THU, FRI, SAT, SUN, M-F, ALL, and DATE. M-F = Monday through Friday. ALL = seven days a week. DATE = Start and End Date fields are enabled so date, rather than day, settings may be used.

Start Time and End Time - These fields define the time period for each timer on a 24 hour clock. The earliest time is 00:00 (midnight) and the latest time is 23:59. Both start time and end time must be on the same day. Time periods will NOT define greater than 24 hours or define across midnight. Any timer with an end time of 23:59 will be automatically extended to midnight to avoid an undefined minute, 23:59 to midnight.

Overnight configurations setup example, If Security Configuration #5 is desired for 20:00 (8 pm) to 6:00 (6 am) Monday through Friday, use two timers and set the day field of both timers to M-F. Set one timer's start time to 20:00 and end time to 23:59. Set the second timer's start time to 00:00, and end time to 06:00. Set configuration # to 5 and the timer status to *ON* for both timers.

CAUTION: Be careful not to define timers that overlap. If the *Start Time* of one timer is earlier than the *End Time* of another timer, they may not operate as expected.

Config. # - This field tells the system which Security Configuration to use in the time period defined by this timer.

Timer Status - Timer Status provides an easy way to turn the timer *ON* or *OFF*. If Timer Status is *OFF*, the timer will be inactive. For example: A timer is set up but not desired currently and turned *OFF*. Later the timer may be turned back *ON* to re-activate it.

Example : To program Security Configuration #4 from 8 am to 4 pm, Monday through Friday.

Step 1: Program Security Configuration #4.

Step 2: Select [9] on the Security Configuration Menu.

Step 3: Select a timer with a status of *OFF*.

Step 4: Use the arrow keys to move the cursor to the column labeled **Day**, press [I] or [D] to change it to M-F.

Step 5: Move the cursor to the **Start Time** hour field, press [I] or [D] to change it to 08.

Step 6: Move the cursor to the **Start Time** minute field, press [I] or [D] to change it to 00. If it is 00 go to the next step.

Step 7: Move the cursor to the **End Time** hour field, press [I] or [D] to change it to 16.

Step 8: Move the cursor to the **End Time** minute field, press [I] or [D] to change it to 00. If it is 00 go to the next step.

Step 9: Move the cursor to **Config. #**, press [I] or [D] to change it to 4.

Step 10: Move the cursor to **Timer Status**, press [I] or [D] to turn *ON.*

Step 11: Press [S] then [Y] to save it.

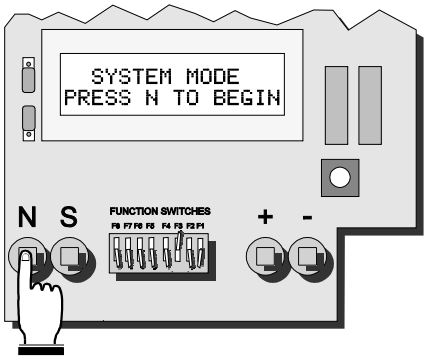
Step 12: Press [ESC] to exit.

4.7 VIEWING AND CHANGING THE SECURITY CODES

The Security code for each floor may consist of one to eight characters, each represented by one of the floor buttons found in the elevator car. **A floor may NOT be *Secured* unless a *Security Code* has been programmed.**

The Appendix titled ELEVATOR SECURITY INFORMATION AND OPERATION provides instructions for elevator passengers on the use of Security operation. Space has been provided for listing the security codes for each floor.

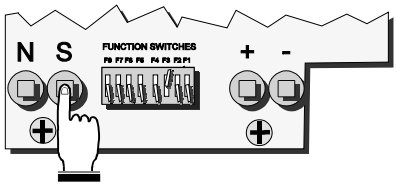
4.7.1 VIEWING THE BUILDING SECURITY MENU - On the MC-PCA Computer board, place the F3 switch in the up position (with all other switches in the down position). The following display appears:



- Press the N push-button.
- The following display will appear:

```
*     BUILDING     *
*  SECURITY MENU   *
```

4.7.2 PROGRAMMING THE SECURITY CODES

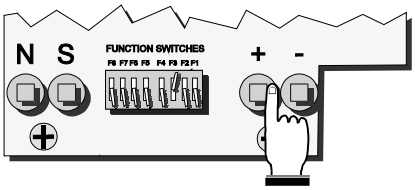


- Press the ***S*** push-button to start programming or changing the Security codes (or to view the codes).
- If no code has been programmed, the computer displays NO CODE PROGRAMMED for that particular floor number. Press the ***S*** push-button again to start programming the Security code.

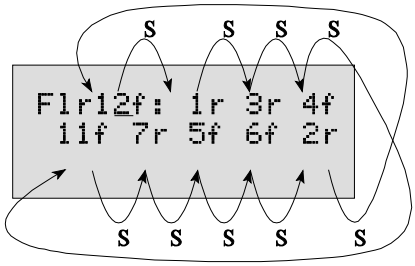
```
Flr 1f: NO
CODE PROGRAMMED
```

- If a code has already been programmed, the computer displays the security code. The cursor will blink below the floor number for the Security code being displayed.

```
Flr 1f: 8r 3f 4f
    2r2lf3lr19f17r
```

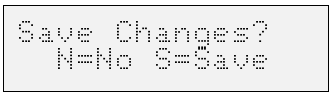


- Press the **+** and – push-buttons to select the floor number to change. The + push-button increments the floor being displayed to the next eligible floor. The – push-button decrements the value.
- Press the ***S*** pushbutton to move the cursor to the first character of the Security code. Press the **+** and – push-buttons to change the value of the first character. Repeat these steps (pressing the S push-button followed by the + and – pushbuttons) until the desired number of characters are programmed (maximum of 8 characters). The S push-button moves the position of the blinking cursor according to the diagram at the right. If any character is left blank, or after all eight characters are programmed, pressing the S pushbutton returns the cursor to the floor number.



- Repeat these steps to program the Security codes for all the floors. You may exit the Building Security Menu at any time during programming by pressing the ***N*** push-button. When the ***N*** push-button is pressed, the LCD will display the following:

- Press the ***S*** push-button to exit or the ***N*** push-button to return to the previous display. If ***S*** is pressed, the following will appear (only if changes have been made):



- Press ***S*** to save the changes or ***N*** to exit without saving (any original codes will remain in effect if the changes are not saved).

4.8 PROGRAMMING CHECKLIST

Use following checklist to ensure that all of the elements required for proper operation of Basic Security with CRT have been programmed. Refer to the listed section for a description and instructions for programming each item.

1. Security Menu Password (Section 4.4).
2. Master Software Key (Section 4.2.1)
3. Security Software Switch (Section 4.2.2)
4. BSI Input, if applicable (Section 4.2.3)
5. Security Configuration Status (Section 4.2.4)
6. Security Configurations, as required (Section 4.5)
7. Security Configuration Timer Table (Section 4.6)
8. Security Codes (Section 4.7)

SECTION 5
ACCESS CONTROL FOR ELEVATORS (ACE)

5.0 GENERAL

This section pertains to Access Control for Elevators (ACE) security. The screens depicted in this section are those found on MCE controllers using Release 4 Communication software. Some screens may look slightly different if your controller is running an earlier version of communication software.

5.1 INTRODUCTION - PRODUCT DESCRIPTION

Access Control for Elevators (ACE) offers the most sophisticated programming capability, including a wide range of options allowing building owners and managers the greatest flexibility of any elevator security system. ACE is implemented in the Simplex Car or Group Supervisor in an M3 Group System. Most of the programming is done through a CRT terminal or PC which can be connected to the controller directly or through a modem.

ACE features include:

- A flexible and easy to program Menu system.
- A user programmable password that regulates access to the ACE Menu system.
- Up to 500 Passenger Access Codes (PAC) can be programmed.
- Four Passenger Groups, each with a programmable Name and a timer table with 16 programmable Time Schedules.
- Eight programmable Security Configurations. The current Security Configuration can be manually selected via the CRT or automatically selected by the Security Configuration Timer Table.
- Sixteen programmable time schedules in the Security Configuration Timer Table. The system can automatically select one of eight Security Configurations.
- A Secured Car Call database stores up to 500 entries. The database is automatically maintained to keep track of when and who entered a car call and the results.

ACE has passenger access codes which allow only authorized passengers access to building floors via the elevators. Each passenger or group of passengers can be assigned a unique access code. Each code can have its own unique set(s) of access permissions. The sets of access permissions can change based on date or day and time using one or more of six time schedules.

General Floor Access Control - Using a CRT terminal or PC, up to eight Security Configurations can be programmed. The Security Configurations allow each floor to be designated as *unsecured*, *secured* or *locked* for car calls and either *unsecured* or *locked* for hall calls. These terms are defined as follows:

- unsecured = unrestricted access, all car and/or hall calls are registered
- secured = access restricted, valid security code required to register car calls
- locked = no access, car calls and/or hall calls are not registered

ACE allows security to be turned ON or OFF, and to determine which of eight Security Configurations is active on any date or day(s) and time, based on a programmable time schedule called the Security Configuration Timer Table.

Floors which have been designated as secured on a Security Configuration *are secured* when that configuration is active and security is ON. In order to gain access to a secured floor via the elevator, a Passenger Access Code (PAC) must be entered using the Car Operating Panel (COP) buttons. The PAC must have permission to access that floor on this day and time. When the COP button for a secured floor is pressed, the button's indicator will flash to indicate that a passenger access code is required. The passenger must enter the code within 10 seconds, otherwise the call will not be registered and the indicator will turn OFF.

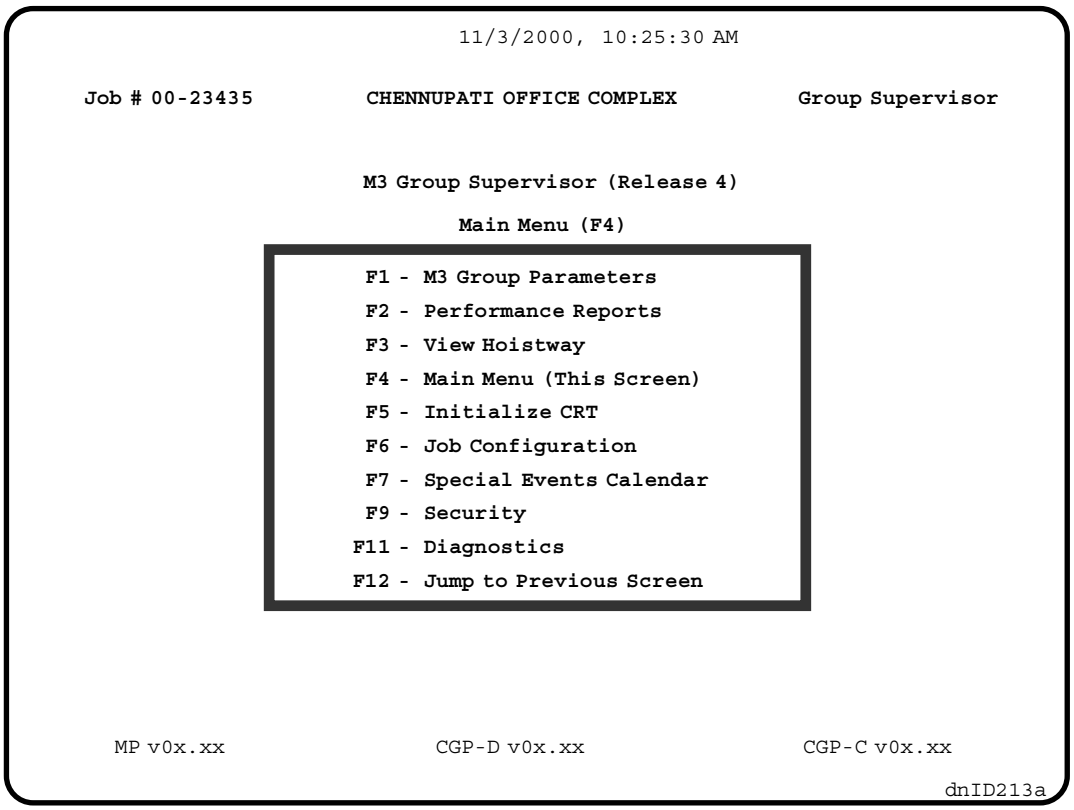
PAC Access Control - Each Passenger Access Code (PAC) can have its own set of access permissions for each floor (access or no access). Each PAC has a Personal Time Schedule which can limit access to a specific date or day(s) and hours. In addition, each PAC can be included in one or more of four groups that have a Group Time Schedule which can limit access to a specific date or day(s) and hours.

Reports - While ACE Security is ON, each time an attempt is made to access a secured floor via the elevators, the date, time, floor, and passenger ID is logged. The 500 most recent attempts are saved and can be viewed and/or printed.

5.1.1 MAIN MENU SCREEN

The CRT terminal's **Main Menu** allows access to the Security Menu using selection F9, Security.

FIGURE 5.1 Main Menu



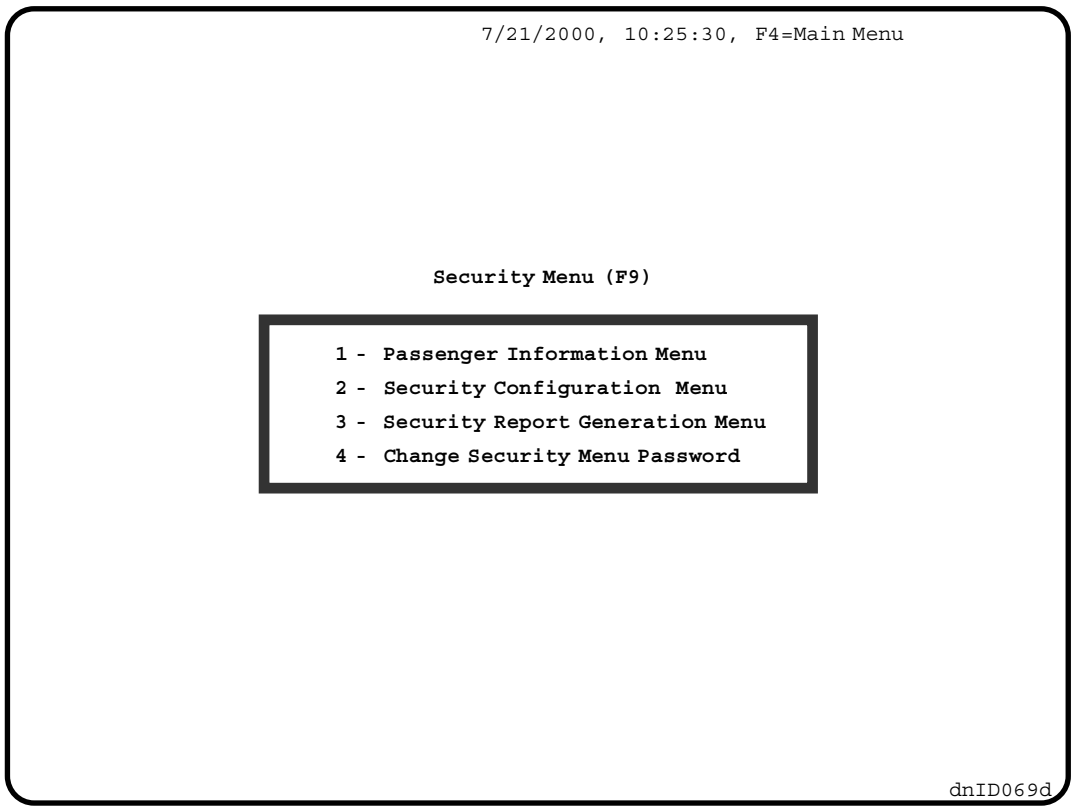
PASSWORD PROTECTED ACCESS TO THE ACE SYSTEM - The Access Control for Elevators (ACE) system is password protected. If no password is programmed, the Security Menu (Figure 5.2) will appear. If a password has been programmed, the following will appear when F9 is pressed:

Security Password:

Type in the password and press ENTER. The password itself will not appear on the screen. Instead, an asterisk (*) will appear for each character typed. When the correct password is entered the Security Menu will appear. Once a valid password has been entered, it is not necessary to re-enter the password unless you exit Security for more than ten minutes.

NOTE: The controller is shipped with no password programmed. Section 5.4 describes how to program or change the password.

FIGURE 5.2 Security Menu (F9) Screen



5.1.2 SECURITY MENU SCREEN

1 **Passenger Information Menu** - Select this menu if you would like to :

- program the Group Time Schedule.
- program the Passenger Information.
- change the size of the PAC.
- edit a Group Name.

2 **Security Configuration Menu** - Select this menu if you would like to :

- program or modify a Security Configuration.
- program or modify the Security Configuration Timer Table.
- change the Current Security Configuration.
- change the Security Software Switch Status.

3 **Security Report Generation Menu** - Select this menu if you would like to :

- see a list of the Secured Car Calls that shows who has entered a car call with the PAC, when it was entered, from which car, to which floor, and if the car call was accepted or rejected.
- clear all the records in the list.

4 **Change the Security Menu Password** - Use this to change the access password.

5.1.3 SECURITY CONFIGURATION MENU SCREEN

The Security Configuration Menu is accessed from the Security Menu by pressing 2. The following is a description of the items on the Security Configuration Menu (see Figure 5.3).

Security Configurations 1 thru 8 can be accessed by pressing 1 - 8. By programming a Security Configuration you can set the security status of each floor for hall calls and car calls. You don't have to program all eight configurations, program only as many as you need. See Section 5.5 of this appendix for programming details.

The **Security Configuration Timer Table**, selection 9, lets you set up a time schedule to turn ACE Security ON and OFF and determine which Security Configuration will be the *current configuration* when the Security Configuration Status is set to *Timed*. Each of sixteen timers can be programmed to select one of the eight Security Configurations. See Section 5.6 for programming details.

Security Configuration Status, selection B, allows manual selection of **Security Configuration #1 - #8** as the *current configuration* , or **Timed** operation. The current status is displayed, i.e. Security Configuration Status: Manual #2, : Timed #3 or : Timed OFF. *Manual #2* means that Security Configuration #2 is the current configuration and it is manually selected. *Timed #3* means that Security Configuration #3 is the current configuration and it is selected via the Security Configuration Timer Table. *Timed OFF* means that Timed operation is selected and that ACE Security is *OFF* because none of the timers in the Security Configuration Timer Table are valid at this time.

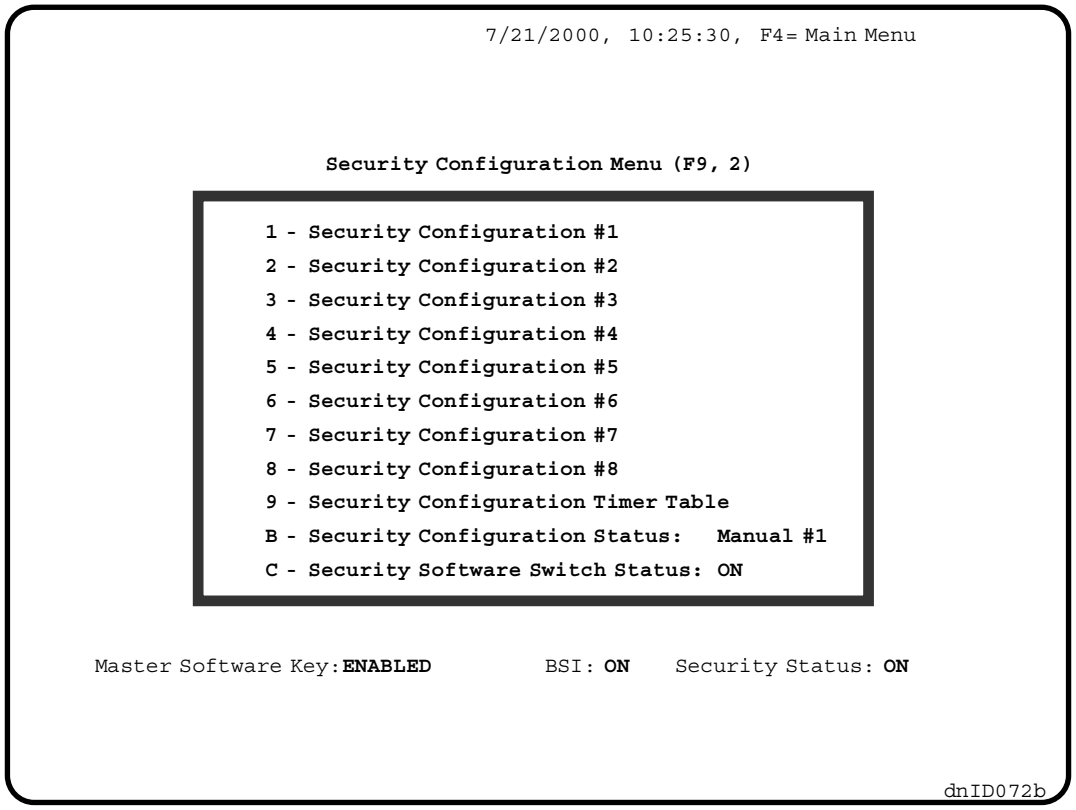
Security Software Switch Status selection C, lets you set the Security Software Switch Status to *ON* or *OFF*. The current status is displayed, i.e. `Security Software Switch Status: ON`. The Security Software Switch Status is one of four elements that determine if ACE Security is ON or OFF (see Section 5.2, Turning ACE Security ON and OFF)

.

Status Line - The line at the bottom of the screen is the status line. The status line contains important, continuously updated information on the status of the Master Software Key, BSI input, and the ACE Security Status (see Section 5.2).

Security Status - The current status of the ACE Security system is displayed next to *Security Status*. It is determined by the status of the Master Software Key, BSI input, Security Software Switch, the Security Configuration Status and, the Security Configuration Timer if in *Timed* operation (see Section 5.2).

FIGURE 5.3 Security Configuration Menu (F9, 2) Screen



5.2 TURNING ACE SECURITY ON AND OFF

There are four elements that determine if ACE Security is ON or OFF. These elements are:

- Master Software Key Status
- Security Software Switch Status
- BSI Input Status (optional)
- Security Configuration Status

The way in which each element affects the Security Status is depicted in the Security Status Decision Matrix (see Table 5.1).

5.2.1 MASTER SOFTWARE KEY STATUS

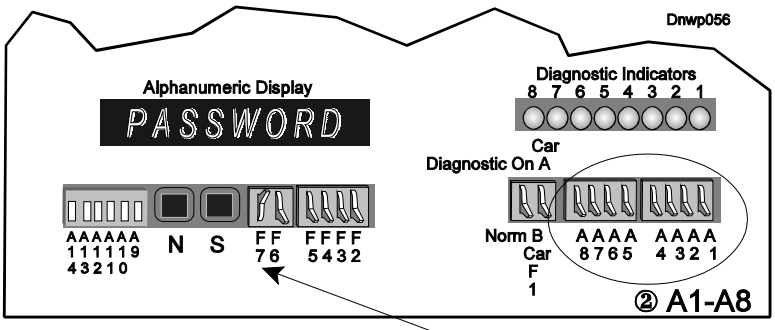
The Master Software Key is a board-level control of the security system mainly for use during periods when the CRT is not operational. The Master Software Key can be set to ***Activated***, ***Deactivated*** or ***Enabled*** through the controller's Computer Swing Panel.

When the Master Software Key is set to *Activated*, the Security Status is ON and Security Configuration #1 is in use. When the Master Software Key is set to *Deactivated*, the Security Status is OFF. When the Master Software Key is set to *Enabled*, the Security Status and the current configuration are determined by the status of the Security Software Switch, the BSI input (optional), and the Security Configuration Status (see Table 5.1, Security Status Decision Matrix).

CHANGING THE MASTER SOFTWARE KEY SETTING - Changes to the Master Software Key setting are made through the controller's Computer Swing Panel in *System Mode.*

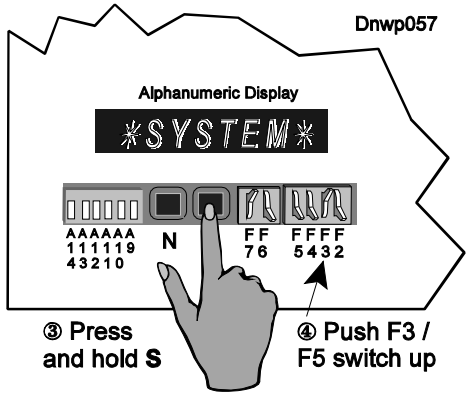
1. Place function switch ***F7*** in the *ON* (up) position. The alphanumeric display shows PASSWORD.

2. Set the A1 - A8 switches to the password value. If no password has been programmed for this job (which is normally the case), set A1 - A8 to OFF (down).



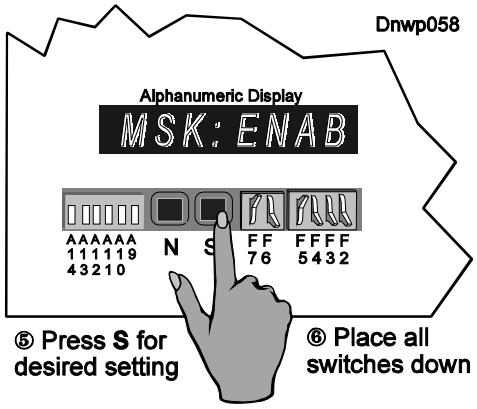
3. Press and hold the ***S*** push button until the alphanumeric display shows *SYSTEM*.The eight vertical status indicators scan from bottom to top. In System Mode, if function switches or pushbuttons are not pressed for two minutes, the computer exits System mode and returns to Normal mode.

4. Place function switch ***F3*** (*F5 on a Simplex Car)* in the *ON*, **up** position, to access the Master Software Key. The alphanumeric screen will display MSK: ENAB, MSK: ACTI, or MSK: DEAC. These are abbreviations for *Enabled*, *Activated*, or *Deactivated* respectively.



5. Press the **S** push button to change the current setting of the Master Software Key.

6. Place the **function switches** in the *OFF*, **down** position when finished. The normal state is *Enabled* so that Security can be controlled via the terminal.



5.2.2 SECURITY SOFTWARE SWITCH

When the Master Software Key is set to *Enabled*, changing the Security Software Switch Status can turn the building's security ON or OFF. Select [C] from the Security Configuration Menu to bring up the following selection line below the menu.

```
Set Security Software Switch: OFF  ON
```

Use [←] or [→] to move the cursor to **ON** or **OFF**, then press [ENTER].

The current status is continuously updated and displayed:

```
C - Security Software Switch Status: ON
```

TABLE 5.1 Security Status Decision Matrix

Inputs or Software Settings				Outputs or Results	
Master Software Key Status	**Security Software Switch Status**	**BSI✶ Input (optional)**	**Security Configuration Status**	**Security Configuration in use**	**Security Status**
Deactivated	n/a	n/a	n/a	none	**OFF**
Activated	n/a	n/a	n/a	1	**ON**
Enabled	ON	n/a	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table
	OFF	OFF	n/a	none	**OFF**
		ON	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table

✶ Ignore the shaded area unless the BSI input is included

5.2.3 BSI

The Building Security Input (BSI) is an input to the controller. It could be a connected to a hardware key-switch that is turned ON or OFF. The status of the BSI input is displayed next to it. Not all systems have the Building Security Input. If your system does not have this input, ignore BSI. Table 5.1 shows how the ACE Security Status is affected by the BSI input.

5.2.4 SECURITY CONFIGURATION STATUS

The current Security Configuration can be selected manually or automatically (Timed). Manual selection means that you manually select one of the eight Security Configurations to be the *current configuration*. Automatic selection means that the current configuration will be determined via the Security Configuration Timer Table. When the Security Configuration Status is *Timed*, the system will search the Security Configuration Timer constantly to achieve automatic selection of the *current configuration*. If none of the timers in the Security Configuration Timer Table is valid for the current day and time, then ACE Security will be OFF. Ace Security can be turned ON and OFF automatically via the Security Configuration Timer Table.

When one of the eight Security Configurations is selected manually, ACE Security is ON if the Master Software Key is Enabled and the Security Software Switch and/or BSI is ON (Table 5.1)

SETTING THE SECURITY CONFIGURATION MANUALLY - To manually select the Security Configuration press [B] in the Security Configuration Menu. The following line will appear under the Menu (the Timed option may not appear):

```
Select Current Configuration:  1  2  3  4  5  6  7  8  Timed
```

Use [←] or [→] to move the cursor or press [1] thru [8]. Select Security Configuration **1** thru **8** and press [ENTER]. The new status will then be displayed:

```
C - Security Configuration Status:  Manual #4
```

SETTING THE SECURITY CONFIGURATION AUTOMATICALLY (TIMED) - If you would like the system to automatically select different Security Configurations for different time periods based on the Security Configuration Timer Table, select [B] from the Security Configuration Menu. The following line will appear below the menu:(The *Timed* option will not be displayed unless at least one Timer in the Security Configuration Timer Table has a *Status* of ON).

```
Select Current Configuration:  1  2  3  4  5  6  7  8  Timed
```

Use [←] or [→] to move the cursor to **Timed** or press [T] and press [ENTER]. The new status will be displayed:

```
C - Security Configuration Status:  Timed #3
```

Timed #3 indicates that Timed mode of operation has been selected and Security Configuration #3 is the current configuration as determined by the Security Configuration Timer Table. If none of the timers in the Security Configuration Timer table are valid at this time, the current time falls between Start Time and End Time and Day includes today, the following will be displayed:

```
C - Security Configuration Status:  Timed OFF
```

5.3 USING THE CRT TO PROGRAM THE ACE SYSTEM

The ACE system must be properly programmed to set up the security for your building's needs. Here are some of the things that need to be programmed before running security on the elevator control system.

- Password for ACE access
- Security Configurations
- Security Configuration Timer Table
- Passenger Information (PAC)
- Group Name
- Group Time Schedules

The following sections will explain how to program them. In this process you will use the following keys:

ENTER to make a selection or to confirm a selection.

ESC to abort or exit an operation, to exit a sub-menu.

1 to 9 to select a particular item from a Menu.

SHIFT used together with a function key to make a selection.

↑ ↓ ← → to move cursor around when programming or scrolling the screen.

TAB to quickly move the cursor from one field to another.

I and D to make changes. I to Increase a value. D to Decrease a value.

S or ALT S to save the changes.

5.4 PROGRAMMING THE ACE PASSWORD

Access to the ACE Security system is password protected. The password may contain up to 8 characters. These characters may be alphabetic or numeric and can include spaces and punctuation. When no password is programmed, access to the Security Menu is unrestricted. No password is programmed when the controller is shipped.

5.4.1 CHANGING THE PASSWORD

To change or program the password, press 4 while the Security Menu is displayed (Figure 5.2). The screen will change to:

```
        Change Security Password (F9, 4)
Enter Current Password:
    Enter New Password:
  Confirm New Password:
```

Type in the current password and press ENTER. The password itself will not appear on the screen when you type it. Instead, an asterisk (*) will appear for each character typed.

Then type in the new password, up to eight characters, and press ENTER. The new password must be typed a second time for confirmation. The new password will not be displayed while being typed. An asterisk (*) will appear for each character typed.

5.4.2 LOST OR FORGOTTEN PASSWORD

If you lose or forget your password, type a question mark '?' at the password prompt and press ENTER. The following will appear on the screen:

```
MCE Security Reference #: xx
```

xx is a number between 0 to 15, randomly generated by the system.

Call MCE Technical Support and tell them the reference number. They will give you a temporary password. Type in the temporary password and press ENTER. If you make a mistake while typing the temporary password, try again. Then choose a new password, enter it and confirm it as described in Section 5.4.1.

5.5 PROGRAMMING THE SECURITY CONFIGURATIONS

A Security Configuration consists of a **Hall Call Map**, an **Auxiliary Hall Call Map** if an auxiliary hallway exists, and several **Car Call Maps**, one for each car (see Figure 5.4). The first column is the floor number displayed in landing labels, followed by columns for the Hall Call Map, Auxiliary Hall Call Map (not shown here), and Car Call Maps. The Auxiliary Hall Call Map will not be shown if the system is not equipped with auxiliary hall calls. The Car Label for each car is displayed on top of the Car Call Map.

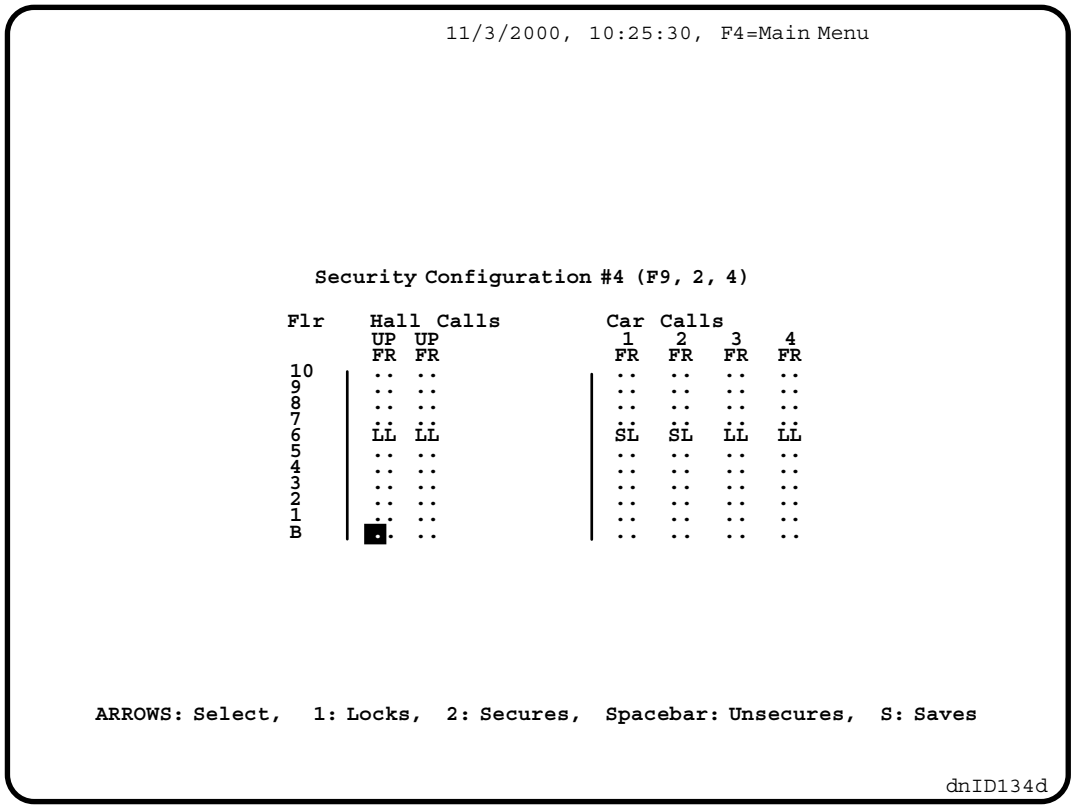
NOTE: Figure 5.5 shows an example of the optional Per-Car Hall and Car Call Mapping.

A floor's security status for ***hall calls*** can be either ***Unsecured*****,** indicated by a '**.**' or ***Locked*****,** indicated by an '**L**'. *Unsecured* for *hall calls* means that access to elevators from that floor is unrestricted. *Locked* for *hall calls* means that access to elevators from that floor is not permitted. The setting can be different for *Up* Hall Calls, column UP, and *Down* Hall Calls, column DN**,** on the same floor. Normally all floors, for hall calls, are unsecured so all hall calls are registered. When a floor is locked for hall calls, no one can leave that floor via the elevator.

A floor's security status for ***car calls*** can be ***Unsecured*****,** indicated by a '**.**', ***Locked*****,** indicated by an '**L**' or ***Secured*****,** indicated by an '**S**'. *Unsecured* for *car calls* means that access to that floor is unrestricted. *Locked* for *car calls* means that access to that floor is not permitted. *Secured* for *car calls* means that access to that floor is permitted only if the valid PAC is entered within ten seconds. If the PAC is correct, has access rights to that floor, and is valid at the current day and time, the car call will be registered.

If there are two different lobbies on the same floor, the floor's security status could be different for calls from different lobbies. The lobbies are symbolized by '**F**' and '**R**' indicating the ***Front*** door lobby and the ***Rear*** door lobby.

FIGURE 5.4 Security Configuration #4 (F9 - F2 - 4) Screen



PROGRAMMING THE HALL CALL AND CAR CALL MAPS - Use arrow keys to move the cursor and use I or D to change the floor security status. When I or D is pressed, the character under the cursor will switch between '**.**', '**L**' and '**S**'.

. = Unsecured — When a floor is Unsecured, all hall calls from the floor and car calls to the floor respond normally.

S = Secured — This status only exists for car calls. When a floor is Secured, access to the floor is restricted and any car call to that floor requires a valid Security Code.

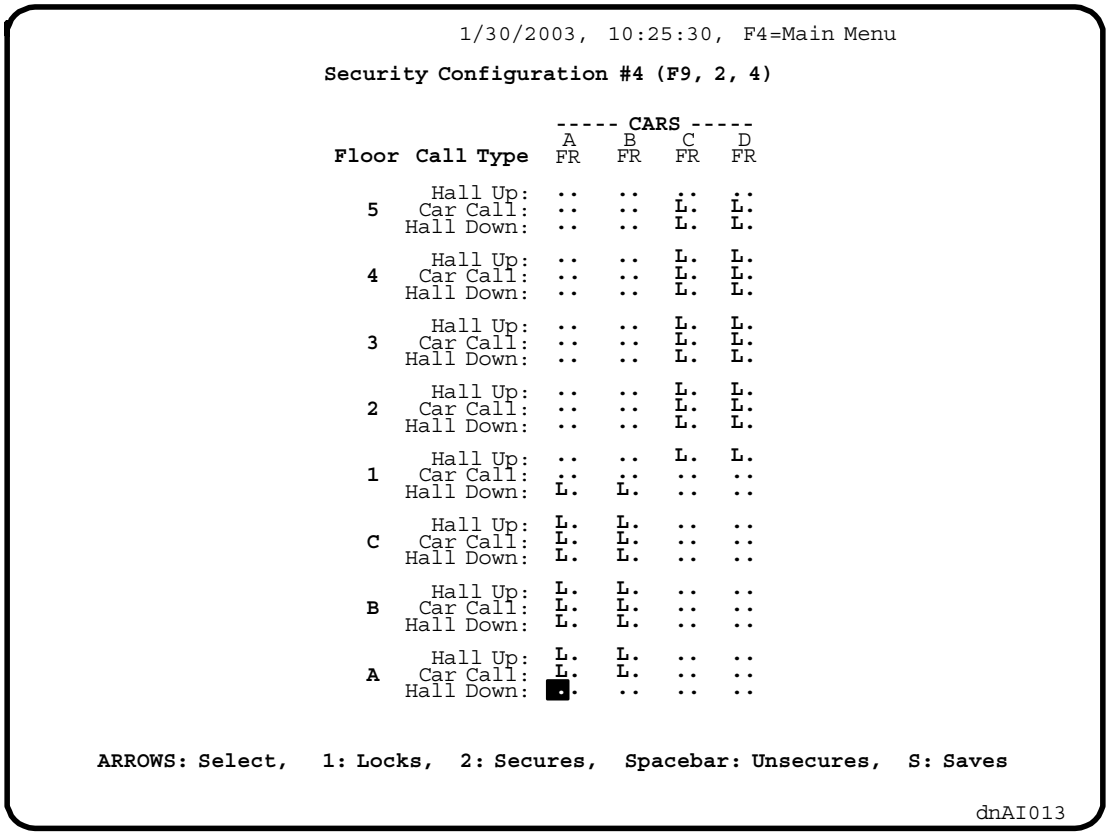
L = Locked — When a floor is Locked, no hall calls or car calls are allowed to be registered. For a hall call, it means no one can leave the floor. For a car call, it means no one can go to that floor.

Use the **arrow keys** or the TAB key to move the cursor from one field to another and use the I and D keys to make changes. When you are ready to save the changes, press S. The system will ignore the S key if no entries were altered. Otherwise, a prompt **`Save changes? (Y/N)`** will appear at the bottom of the screen, press Y to confirm the save.

Press N to not save the changes.

PER-CAR HALL AND CAR CALL MAPPING - If so ordered from the factory, your system may offer Per-Car Hall Call Security. Without Per-Car Hall Call Security, only car calls are configured on a per-car basis as shown in Figure 5.4. With Per-Car Hall Call Security, *both* hall and car calls may be configured on a per-car basis as shown in Figure 5.5.

FIGURE 5.5 Optional Per-Car Hall and Car Call Mapping



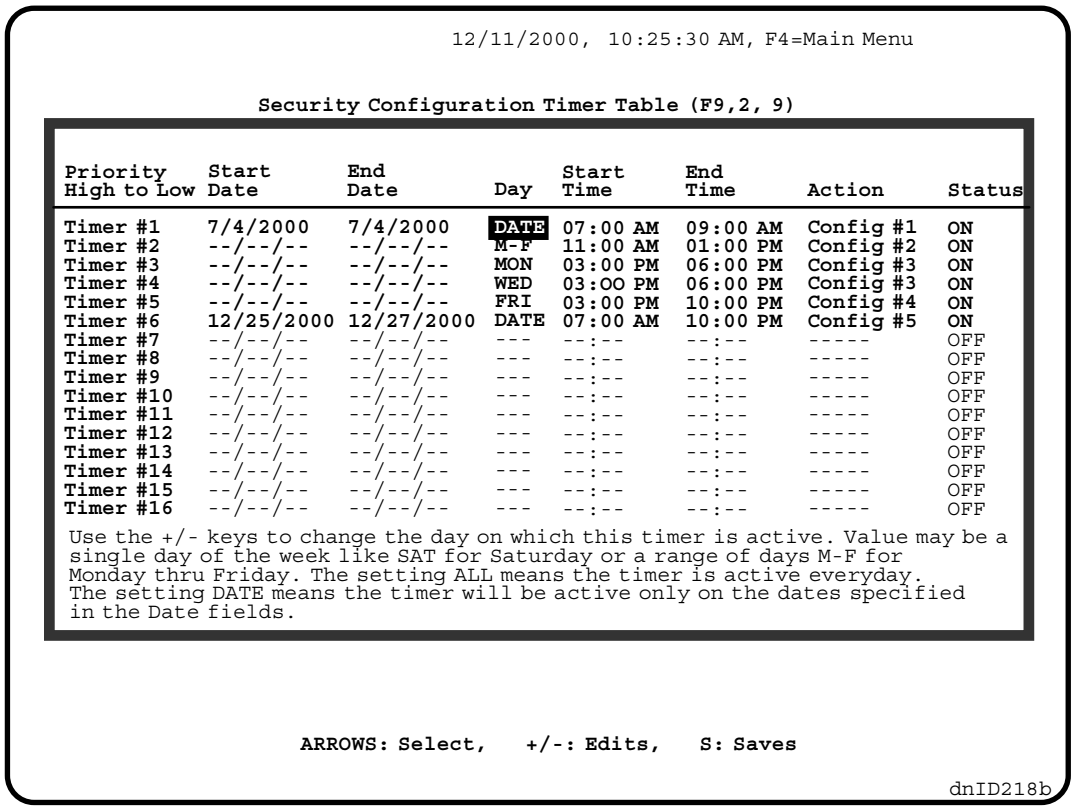
5.6 PROGRAMMING THE SECURITY CONFIGURATION TIMER TABLE

The Security Configuration Timer Table has 16 time schedules, Timer #1 thru #16. Each timer has a column for ***Start Date, End Date, Day***, ***Start Time***, ***End Time***, ***Action***, and ***Status***. The timers can be programmed to specify which Security Configuration will be the current configuration based on the date or day of the week, starting at Start Time and ending at End Time. The timer itself can also be set to *ON* or *OFF*, in use or not in use, via the Status.

When Master Software Key Status is *Enabled* and the BSI and/or the Security Software Switch Status is *ON*, and the Security Configuration Status is *Timed*, the controller will search the Security Configuration Timer Table for a timer with a Status of *ON*. The controller will then compare the current day and time with the day and time period defined in the timer. The highest priority timer found that has a defined day and time period into which the current day and time falls will be the active timer. The current configuration will be determined by the setting under ***Action*** in the active timer. The timers are searched continuously to achieve automatic switching of configurations.

> **NOTE:** If no timers are found with a defined day and time period into which the current day and time falls, the Security Configuration Status will be **Timed OFF** and the Security Status will be **OFF**.

FIGURE 5.6 Security Configuration Timer Table (F9, 2, 9) Screen



To program the Security Configuration Timer Table, press 9 at the Security Menu. The Security Configuration Timer Table screen will appear, as shown in Figure 5.6. All 16 timers (time schedules) are displayed and can be programmed on this screen. Each timer has seven programmable fields: ***Start Date, End Date, Day***, ***Start Time***, ***End Time***, ***Action***, and ***Status***. Timer #1 has highest priority and Timer # 16 has lowest priority. A timer's Status must first be changed to ON before other fields can be edited.

EDITING METHODS - Use the **arrow keys** to select (highlight) the parameter to be edited. Instructions for editing appear at the bottom of the window. The method of editing varies depending on the selected field, i.e. when the Day, Action or Status fields are selected the **Space Bar** can be used to scroll through the available options or the **I** / **D** or **+** / **-** keys can be used to increment or decrement the value. The Date field is only editable if the Day field is set to DATE.

When the Start Time or End Time fields are selected, press **Enter** to edit and then type the new value. Most of the standard text editing keys are functional. Use the **Arrow** keys to select a character and type a new value over the old value. The **Insert** key toggles type-over and insert modes. The **Delete** key deletes the next character. The **Home** key moves the cursor to the far left and the **End** key moves the cursor to the far right. Press **Enter** when you have finished editing or **Esc** to cancel the edit.

SAVING THE CHANGES - Edited parameter values do not become effective until they are *saved*. Save the changes by pressing the **S** key. A message, **`Save changes? (Y/N),`** is displayed. Press **Y** to save or **N** to not save and continue editing. If you exit the screen without saving, the message, **`Save changes? (Y/N)`**, is displayed. Press **N** to exit without saving the changes. If **Y** is pressed, a confirmation message, **`Save Complete`**, is displayed. If there is a problem the message **`*** ERROR Saving Parameters ***`** is displayed. Contact MCE Technical Support for assistance.

The following is a description of the possible values for each field in the Security Configuration Timer Table:

Start Date and End Date - These fields specify the dates on which this timer will be active. To edit these fields, the Day field must be set to DATE.

Day - Day specifies the day or days of the week. There are ten choices: MON, TUE, WED, THU, FRI, SAT, SUN, M-F, ALL and DATE. M-F means Monday through Friday. ALL means all seven days of a week.

Start Time and End Time - These fields define the time period for each timer. The hour ranges from 0 to 23, and the minute ranges from 0 to 59. The earliest time is 12:00 AM (00:00) and the latest time is 12:00 AM (00:00). An End Time of 12:00 AM (00:00 means the timer stays active until the end of the day. Both start time and end time must be in the same day. No time period can be defined greater than 24 hours or defined across midnight.

For example, suppose you want to use Security Configuration #5 overnight, 8:00 PM (20:00) to 6:00 AM (06:00) Monday through Friday. Use two timers and set the Day field of both timers to M-F. Set one timer's start time to 8:00 PM (20:00) and end time to 12:00 AM (00:00). Set the second timer's start time to 12:00 AM (00:00), and End Time to 6:00 AM (06:00). Set Action to Config #5 and Status *ON* for both timers.

CAUTION: Be careful not to define timers that overlap. If the *Start Time* of one timer is earlier than the *End Time* of another timer they may not operate as you expect.

Action - This field tells the system which Security Configuration to use in the time period defined by this timer.

Status - Status provides an easy way to turn a timer ON or OFF. If the Status is OFF, the Timer will not be used. If you set up a timer and for some reason you decide not to use it now, just turn the Status to OFF. Later when you want to use it again, set its status to ON.

Example : You would like the system to use Security Configuration #4 from 8 am to 4 pm, Monday through Friday.

Step 1: Program Security Configuration #4.

Step 2: Select 9 on the Security Configuration Menu.

Step 3: Find a free timer and set the **Status** to *ON.*

Step 4: Set the **Day** to M-F.

Step 5: Set the **Start Time** to 8:00 AM (08:00).

Step 7: Set the **End Time** to 4:00 PM (16:00).

Step 9: Set the **Action**, to Config #4.

Step 11: Press S then Y to save it.

Step 12: Press ESC to exit.

Repeat these steps to program other timers.

5.7 ASSIGNING THE PASSENGER ACCESS CODES (PAC)

The Passenger Access Code (PAC) is the code assigned to and used by a passenger, or a group of passengers, to gain access to *Secured* floors via the elevator when ACE Security is ON. Passenger Access Codes are assigned by entering passenger information into the PAC database. The following five elements make up a single record in the PAC database: the **Passenger Name**, the **Passenger Access Code**, a **Floor Map**, a **Personal Time Schedule** and a **Group Assignment Table**. The maximum number of records in the PAC database is dependent on the equipment and the memory available, typically 500.

Passenger Name, the *key field* in the PAC database, is the name of the person to whom the PAC is assigned. When ACE Security is ON, every time the PAC is entered, the Name will be recorded in the Secured Car Call data base to identify the person who has used the PAC.

Passenger Access Code is the code entered with the car call to gain access to a Secured floor. The PAC consists of a series of landing labels. The size of the Code (number of landing labels) can be changed to meet your needs. Its default value is 2, when the system is shipped. The maximum value is 8. All PAC's in the system must be the same size.

The **Floor Map** is used to grant or restrict floor access rights. ACCESS means the PAC's user has access rights to that floor. NO ACCESS means the PAC's user does not have access rights to that floor.

Personal Time Schedule - Even with the Floor Map set to "ACCESS," the PAC may not be allowed access because of another restriction - **Time**. Each PAC has a Personal Time Schedule, and in addition, it can be assigned to any of four Groups, each of which has a

Group Time Schedule. The Personal Time Schedule has four independent timer's to tell the system when this PAC can be used. Each timer has a Date, Day of the week, Start Time, End Time, and Status (ON/OFF). The PAC can only be used on that day or days of the week, after Start Time and before the End Time. With the Timer Status OFF, the timer will not be used. If all four timers are OFF, the PAC may not be used at all, unless it has been assigned to a Group and the time period defined in the Group's Timer Table includes the current time.

Group Assignment Table is used to assign the PAC to any of four groups. Each group has a Group Timer Table which is similar to the Personal Time Schedule, except that it has 16 timers. If a PAC belongs to a group, the group's Timer Table will be used as a supplement to the PAC's Personal Time Schedule.

5.7.1 PASSENGER INFORMATION MENU SCREEN

The Passenger Information and Group Timer Tables are programmed using selections from the Passenger Information Menu. From the Security Menu, select the Passenger Information Menu by pressing 1 (Figure 5.7). The following selections are available from the Passenger Information Menu:

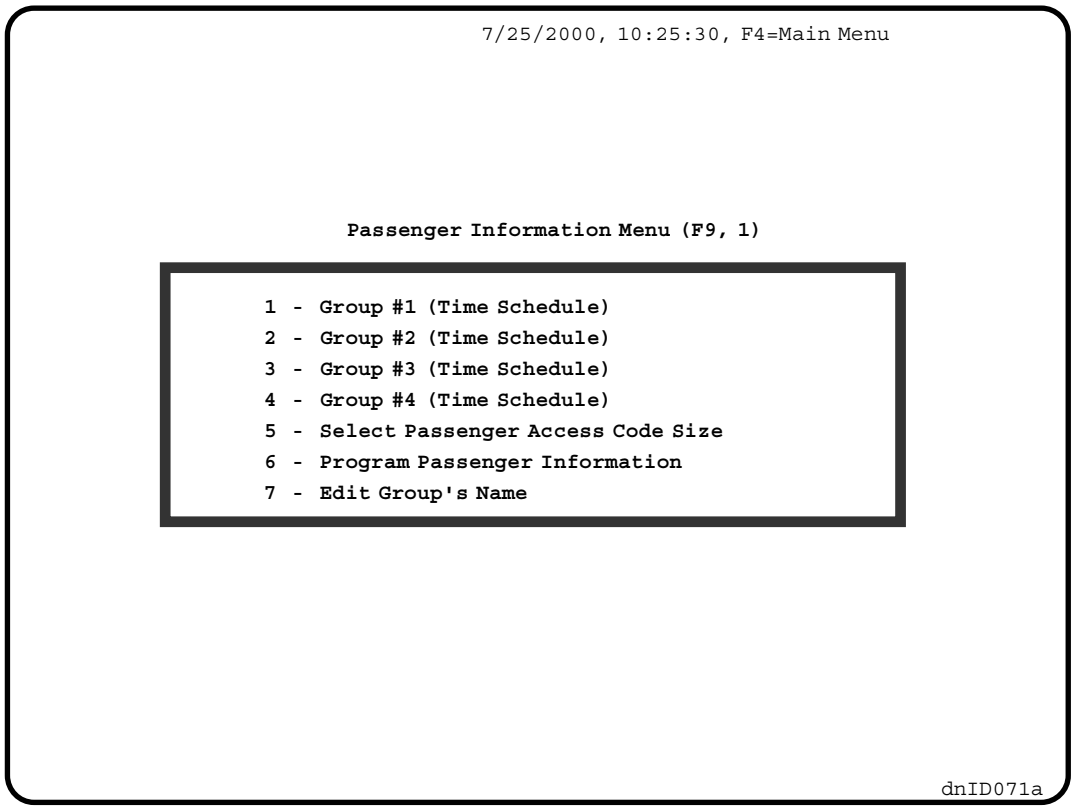
1 - 4 are used to **program the Group Timer Tables** (see Section 5.10).

5 **Passenger Access Code Size**, lets you set the size of the PAC.

6 **Program Passenger Information**, lets you add, delete or modify PAC records.

7 **Edit Group Name**, lets you modify the Group's name. The Group Name is followed by "(Time Schedule)" on the Passenger Information Menu.

FIGURE 5.7 Passenger Information Menu (F9 , 1) Screen



5.7.2 CHANGING THE PAC SIZE

The PAC size defines how many characters (landing labels) a Passenger Access Code contains. The size range is from 2 to 8. The default value is 2 when the controller is shipped. All the PACs in the system must be the same size.

To change the PAC size press 5, Select Passenger Access Code Size, at the Passenger Information Menu. The following message will appear beneath the menu.

```
Enter Passenger Access Code Size:   2
```

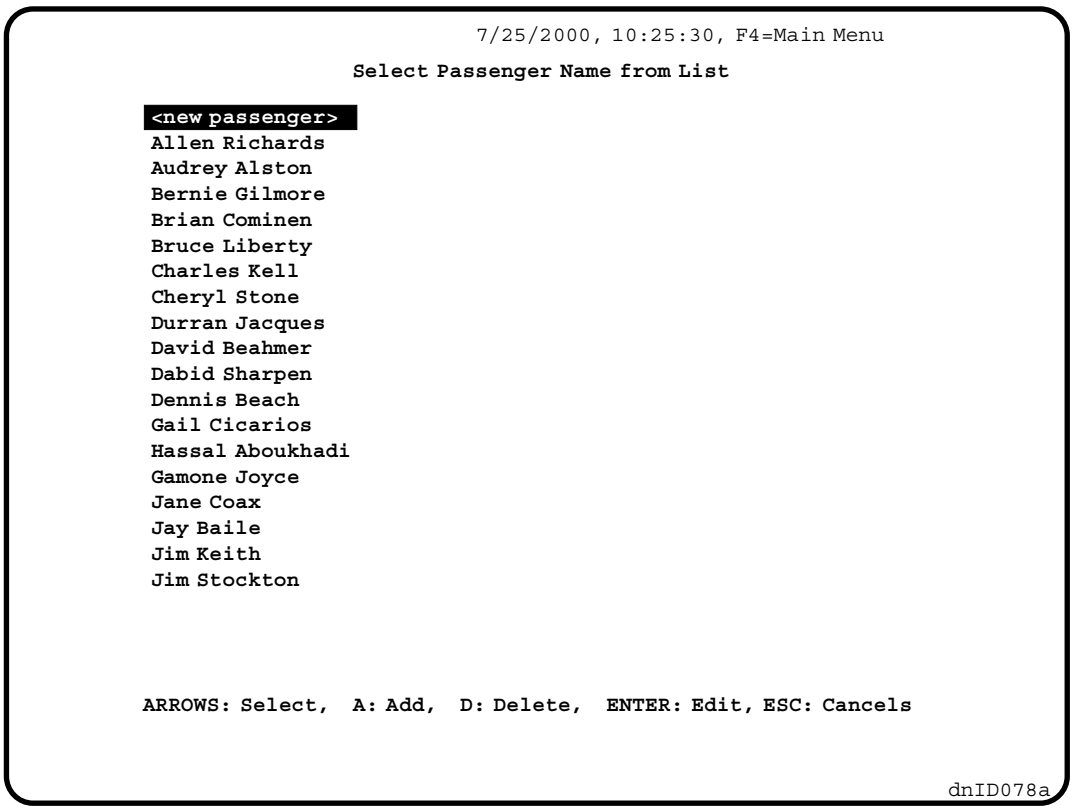
Press I or D to increase or decrease the size. The new size is effective immediately.

CAUTION: The PAC Size should be set before you start to do any Passenger Information programming. The PAC size should not be modified while the ACE Security is ON.

5.7.3 ENTERING PASSENGER INFORMATION INTO THE PAC DATABASE

Passenger Information is stored in the PAC database. The maximum number of records in the database is dependent on available memory, usually 500 or 1000 records. Each PAC record has 5 fields; **Name**, **PAC**, **Personal Time Schedule**, **Floor Map** and **Group Assignment Table**. Once at lease one passenger name has been entered using the Passenger Information Editing screen, pressing 6 on the Passenger Information Menu brings up the Passenger Name List screen shown in Figure 5.8.

FIGURE 5.8 Passenger Name List (F9, 1, 6) Screen



All the names currently in the PAC database are listed here. They are sorted in alphabetical order. Each name is associated with one PAC record. In other words, you choose the PAC record to edit by selecting the name that is associated with it. Use ↑ or ↓ arrow keys to scroll through the list. For fast scrolling use PG↑ or PG↓ keys.

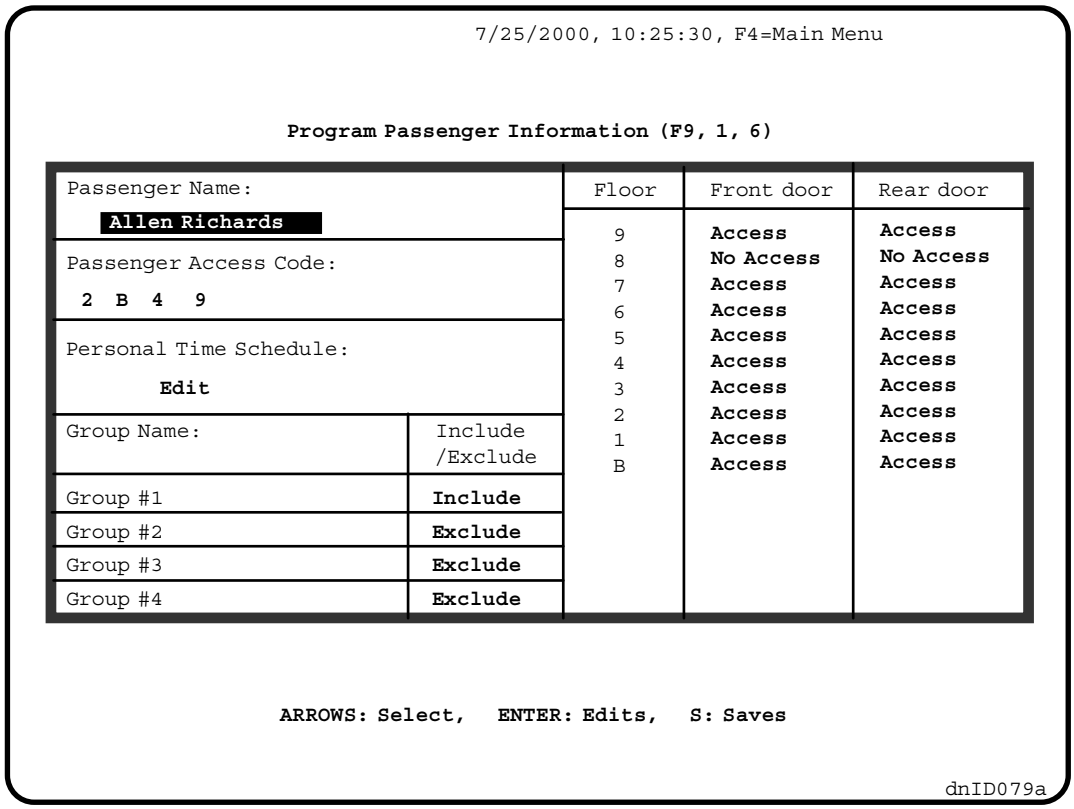
Initially there may be no names listed, the database contain no records. You can **Add, Delete** or **Edit** PAC records. Press A to Add a record, D to Delete a record or E to Edit a record. If you press A to Add a record or ENTER to Edit a record, the Passenger Information Editing screen will be displayed (Figure 5.9).

PASSENGER INFORMATION EDITING SCREEN - The Passenger Information Editing screen, shown in Figure 5.9, has 5 sections corresponding to five fields in a PAC record. Use the TAB key to move between fields. You can save your changes at any time during programming, or you can save them after you finish modifying all the fields.

To save the changes at any time while in the Passenger Information Editing screen, press S. The system will do nothing if you didn't make a change. Otherwise, a prompt **`Save changes? (Y/N)`** will appear at the bottom of the screen. Press Y to save. Press N to not save the changes.

When you are finished editing all of the fields, press the ESC key to exit. If you've made some changes and have not saved them, a prompt **`Save changes? (Y/N)`** will appear at the bottom of the screen. Press Y to save and exit. Press N to not save and exit.

FIGURE 5.9 Program Passenger Information (F9, 1, 6) Screen



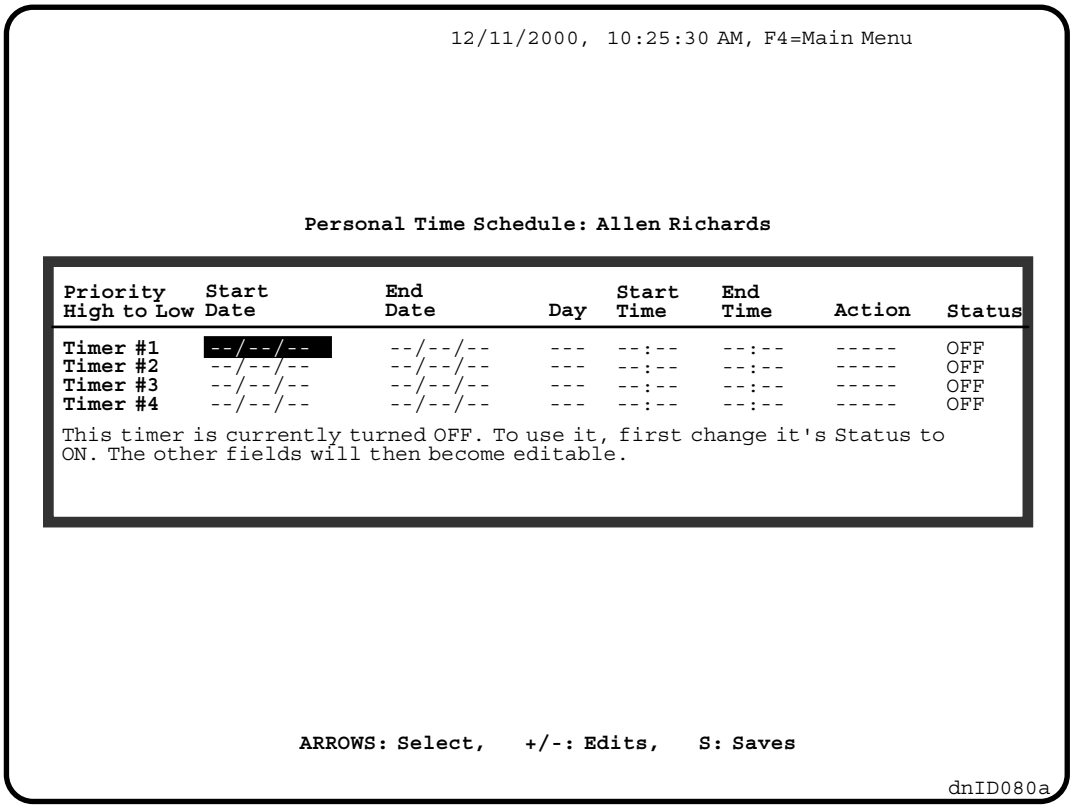
PASSENGER NAME - The Passenger Name field, at the top left of the screen, is the *key field* of the PAC database. The name here is the one you will see on the Passenger Name List and also on the Secured Car Call report. The Name may contain up to 16 characters. These characters may be upper and lower case, alphabetic or numeric, and may include spaces and punctuation. The only restriction is that an asterisk (*) cannot be use as the first character of the name.

Type a new name or press **Enter** to edit the existing name. Most of the standard text editing keys are functional. Use the **Arrow** keys to select a character and type a new value over the old value. The **Insert** key toggles type-over and insert modes. The **Delete** key deletes the next character. The **Home** key moves the cursor to the far left and the **End** key moves the cursor to the far right. Press **Enter** when you have finished editing or **Esc** to cancel the edit.

PASSENGER ACCESS CODE (PAC) - The Passenger Access Code (PAC) is a combination of the landing labels. The number of landing labels you see here is the same as the size of the PAC, which was set in Section 5.7.2. To program the PAC, use ← or → arrow key to move the cursor, use I or D to change each label.

PERSONAL TIME SCHEDULE - The Personal Time Schedule defines the time restrictions for the PAC. The Time Schedule tells the system on which day of the week, *from* what time *to* what time this PAC is valid. Four time periods can be defined. To program the Personal Time Schedule, press TAB until *Edit* is highlighted and press ENTER. The Personal Time Schedule screen (Figure 5.10) will be displayed. Use ← or → or ↑ or ↓ arrow keys to move the cursor, use I or D to change each item. If you exit without saving, a prompt: **`Save changes? (Y/N)`** will appear at the bottom of the screen. Press Y to save or N to not save the changes.

FIGURE 5.10 Personal Time Schedule Screen



GROUP NAME - The Group Name field lists the groups to which this PAC belongs. All four groups are named on the left side of the table (see Figure 5.9). The assignment status is displayed on the right. To assign the PAC to a group, change the status to **Include**. **Exclude** means the PAC is not assigned to the group. If the PAC is included in a group, that group's Time Schedule will be used to supplement the PAC's Personal Time Schedule. This means that the Group Time Schedule(s) will be used to validate the PAC if the current time doesn't fall into any time periods defined in the Personal Time Schedule. Use ↑ or ↓ arrow keys to move the cursor and I or D to make the change.

FLOOR MAP - The right half of the Passenger Information Editing screen (Figure 5.9) shows the Floor Map field. The Floor Map is used to assign access rights to the PAC. The first column is the Floor name displayed as the Landing Label. The next two columns show the access rights for the front door and the rear door for each floor. **Access** means the PAC has access rights. **No Access** means that access rights are not granted.

Use the arrow keys to move the cursor and I or D to make the change. If the building has more floors than can be shown on a single screen the PG↑ and PG↓ keys can be used for fast scrolling to view and program other floors.

ADD A RECORD - At the Passenger Name list screen shown in Figure 5.8 press A to add a PAC record. The screen will change to the Passenger Information editing screen. The name field will be empty and the other fields will have their default values. Type in the Name and program all the fields as described above. After you have programmed all the fields and saved the record, press the ESC key to return to the Passenger Name list screen.

EDIT A RECORD - At the Passenger Name list screen, use the arrow key to select the name associated with the record you would like to edit and press ENTER. The screen will change to the Passenger Information editing screen (Figure 5.9). The data in the record will be displayed. When you have finished editing, Press S to save the changes and Y to confirm, then press the ESC key to return to the Passenger Name list screen.

DELETE A RECORD - At the Passenger Name list screen, use the arrow keys to select the name associated with the record you would like to delete, then press D. You will be prompted for confirmation. `Delete record for passenger "Jane Doe" (Y/N)?` will appear. Press Y to confirm the deletion, or press N to abandon the deletion.

5.8 PROGRAMMING THE GROUP TIME SCHEDULES

A passenger, and his or her Passenger Access Code (PAC), can be assigned to any of four groups. The groups are listed on the Passenger Information Menu (Figure 5.9). The Group Names may be customized (see section 5.8.1). Each group has an associated Time Schedule. A Group Time Schedule has 16 timers so up to 16 time periods can be defined. These time periods act as additions to the time periods defined in the passenger's Personal Time Schedule. When determining access rights, the controller first checks the passenger's Personal Time Schedule. If current time does not fall into any of those time periods, the controller will check the Group Time Schedule for any groups to which the passenger has been assigned.

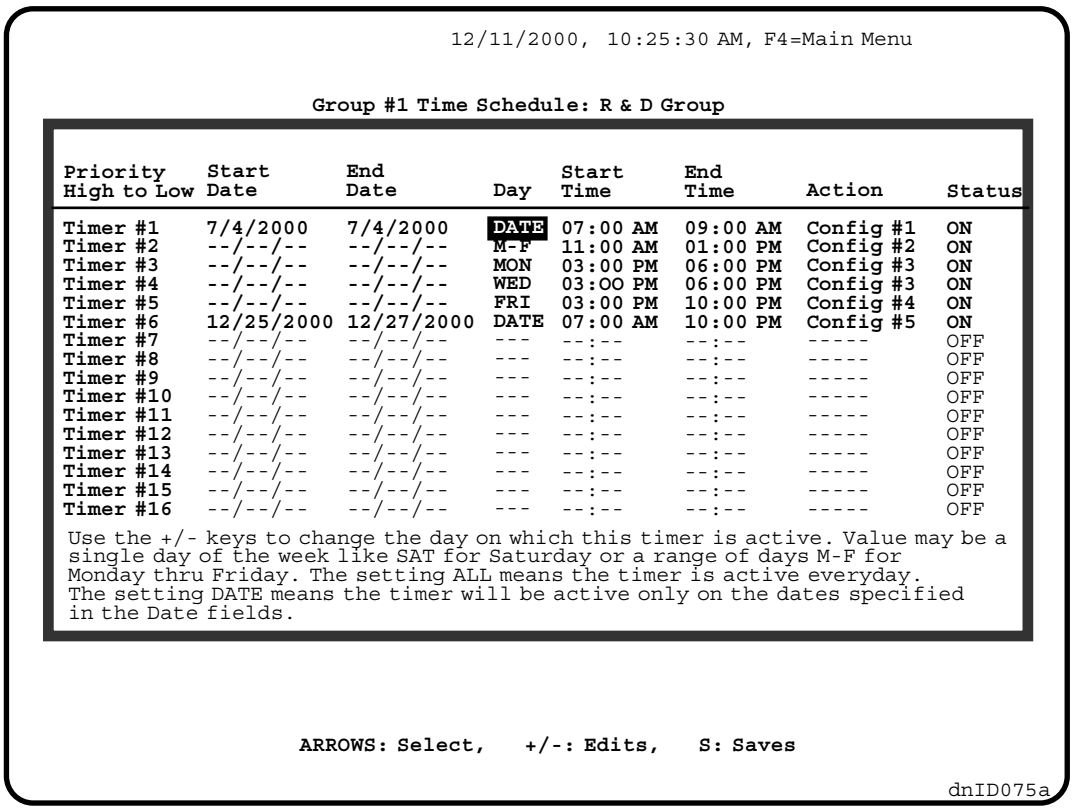
To program a Group Time Schedule, press the function key shown in front of the group name on the Passenger Information Menu. The Group Time Schedule screen will be displayed (Figure 5.10).

All 16 timers are displayed and programmed on this screen. Each timer has six programmable fields, ***Start Date, End Date, Day***, ***Start Time***, ***End Time*** and ***Timer Status***. Use arrow keys or the TAB key to move the cursor from one field to another and use I or D to make the change.

Press S any time you want to save the change. The system will do nothing if no change has been made. Otherwise, a prompt `Save changes? (Y/N)` will appear at the bottom of the screen. Press Y to save or N to not save the changes.

When you finish programming, press the ESC key to exit. If you exit without saving, a prompt: `Save changes? (Y/N)` will appear at the bottom of the screen. Press Y to save or N to not save the changes.

FIGURE 5.10 Group Time Schedule (F9, 1, 1) Screen



The following is a description of possible values for each field:

Start Date and End Date - These fields specify the dates on which this time schedule will be active. To edit these fields, the Day field must be set to DATE.

Day - Day specifies the day or days of the week. There are ten choices: MON, TUE, WED, THU, FRI, SAT, SUN, M-F, ALL and DATE. M-F means Monday through Friday. ALL means all seven days of a week.

Start Time and End Time - These fields define the time period for each time schedule. The hour ranges from 0 to 23, and the minute ranges from 0 to 59. The earliest time is 12:00 AM (00:00) and the latest time is 12:00 AM (00:00). An End Time of 12:00 AM (00:00 means the timer stays active until the end of the day. Both start time and end time must be in the same day. No time period can be defined greater than 24 hours or defined across midnight.

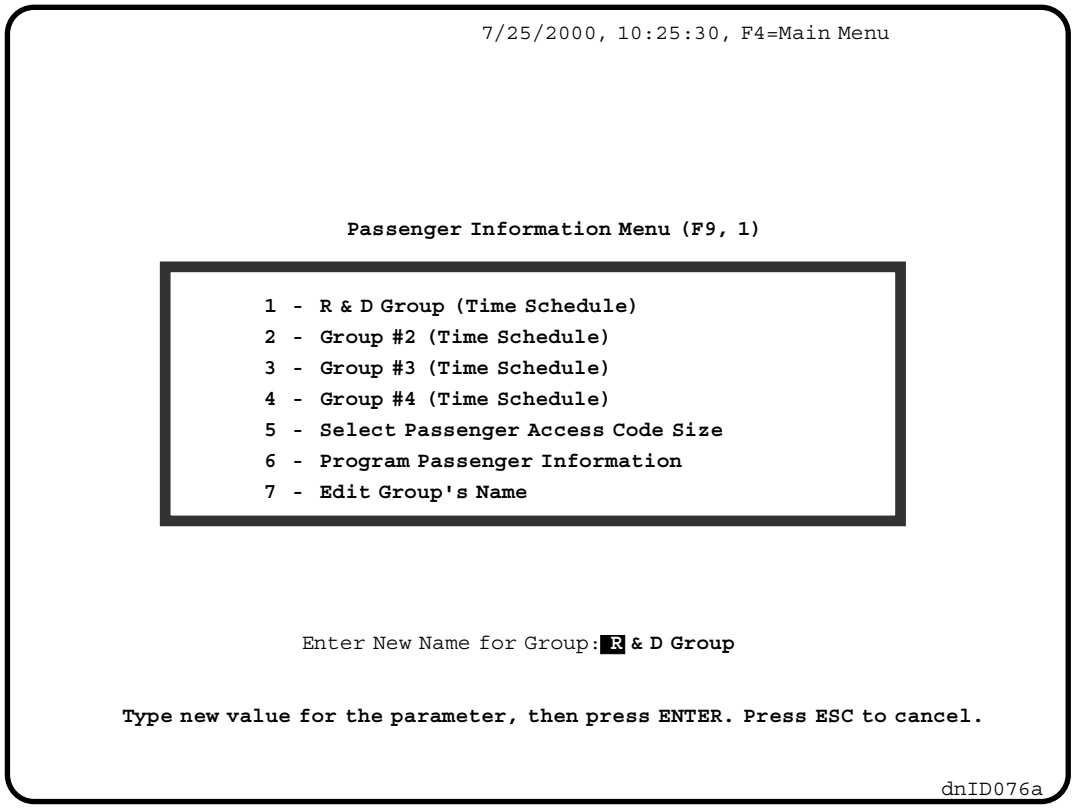
Status - provides an easy way to turn the timer ON or OFF. If the Status is OFF, the Time Schedule will not be used. If you set up a time schedule and for some reason you decide not to use it now, just turn the Status to OFF. Later when you want to use it again, set its status to ON.

5.8.1 CHANGING A GROUP NAME

The Group Name is used to identify each group. The first four items on the Passenger Information Menu are the Groups and the names are followed by (Time Schedule). The Group Names can be changed, for example, to the name of a department in your organization or an organization in your building.

To change a Group Name, press 7 on the Passenger Information Menu screen. A selection line will appear beneath the Menu. Use left or right arrow keys to move the cursor and press ENTER to make the selection. The Group's name will appear in the box for you to modify. See Figure 5.11.

FIGURE 5.11 Passenger Information Menu (F7 - F1) Screen



Type in the new name, up to 25 characters, upper and lower case alphabetic or numeric including spaces and punctuation. Use the ← or → arrow keys to move the cursor and type the new characters over the old ones. The Insert and Delete keys are not functional here. Use the space bar for blank characters.

When you have finished editing, press ENTER to save the change. The system will do nothing if you didn't make any change. Otherwise, a prompt **`Save Complete`** will appear at the bottom of the screen to confirm the save.

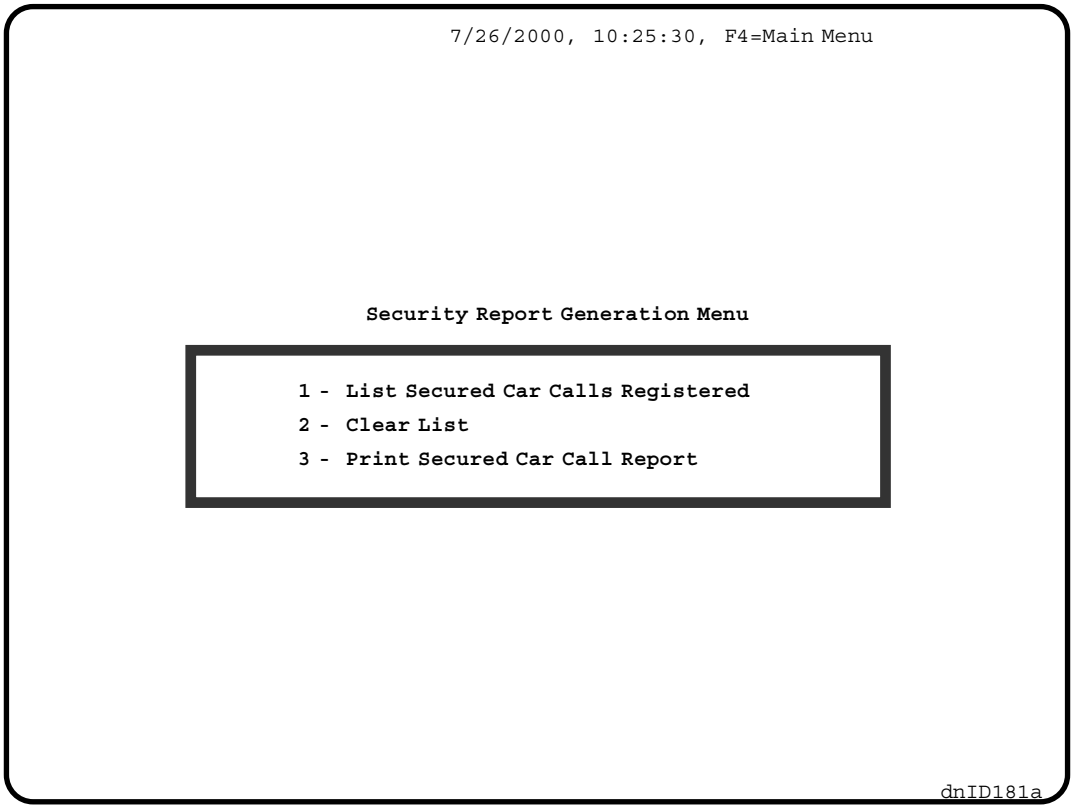
5.9 SECURITY REPORTS

Whenever the ACE Security is ON, all the car calls to the Secured floors are recorded into a database in the memory. The database can hold up to 500 records. When the database is full, a new record will replace the oldest one in the database. The database will always contain a record of the latest 500 Secured car call. After you have viewed the records in the database, you can leave the database as it is or you can delete all the records.

5.9.1 VIEWING THE SECURED CAR CALL LIST

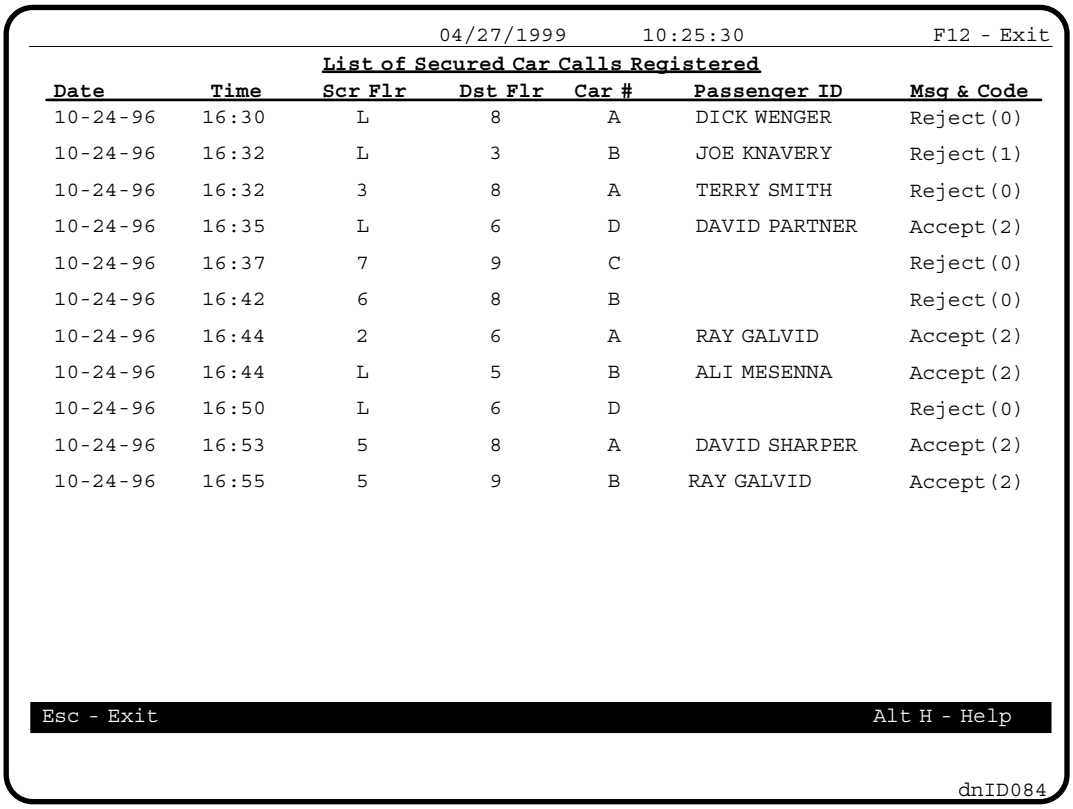
With the Security Menu displayed, pressing 3 will bring display the Security Report Generation Menu shown in Figure 5.12.

FIGURE 5.12 Security Report Generation Menu (F9, 3) Screen



Press 1 in the Security Report Generation Menu and the screen shown in Figure 5.13 will appear.

FIGURE 5.13 List Secured Car Calls Registered (F9, 3, 1) Screen



For each record, the list shows the date and time the car call was entered. The items in the column labeled **Src Flr** are the source floors where the calls were entered and the items in the column labeled **Dst Flr** are the destination floors. The numbers under the **Car #** column are the labels of the cars where the call was entered. The **Passenger ID** is the name associated with the PAC that was used with the call. Some of the ID fields are blank because non-existent PAC's had been entered with those car calls. The **Msg & Code** shows the action the system had taken for that car call and why.

NOTE: When a passenger is deleted, any entries for that passenger on the report are shown with the leading character of the ID replaced with an asterisk (*),

To view the report use ↑ and ↓ to scroll one line at a time or use PG↑ and PG↓ to scroll pages.

Message and Code for Secured Car Calls

Reject (0) REJECTED because of the non-existence of PAC.

Reject (1) REJECTED. The PAC has no access right to the destination floor.

Accept (2) ACCEPTED. The PAC exists, has access right to the floor and the time when the PAC was entered was a valid time based on the Personal Time Schedule.

Accept (3) ACCEPTED because the PAC exists, has access right to the floor and the time when the PAC was entered was a valid time based on the Group Time Schedule of the group the PAC belongs to.

Reject (4) REJECTED. Even though the PAC exists, has access right to the floor and it belongs to the group, the time when the PAC was entered is neither within the time periods defined in PAC's Personal Time Schedule nor the time periods defined by the Group Time Schedule.

Reject (5) REJECTED. Even though the PAC exists and has access right to the floor, the time when the PAC was entered was not within the time periods defined in the PAC's Personal Time Schedule and the PAC does not belong to any group.

5.9.2 CLEARING THE RECORDS OF REGISTERED CAR CALLS

To clear the database press 2 in the Security Report Generation Menu. You will see the next two lines displayed on the screen:

```
All events logged in the list will be deleted
Press ENTER to clear list or any other key to continue
```

Pressing the ENTER key at this time will clear all the records and reset all indexes internally to get ready to record the new car calls. If you pressed 2 by mistake, press any other key to abort the operation.

5.9.3 PRINTING THE SECURED CAR CALL REPORT

From the Security Report Generation Menu select 3, Print Secured Car Call Reports. Follow the instructions presented on the screen.

5.10 PROGRAMMING CHECKLIST

Use the following checklist to ensure that all of the elements required for proper operation of Access Control for Elevators (ACE) Security have been programmed. Refer to the listed section for a description and instructions for programming each item.

1. ACE Password (Section 5.4).
2. Master Software Key - Enabled (Section 5.2.1)
3. Security Software Switch (Section 5.2.2)
4. BSI Input, if applicable (Section 5.2.3)
5. Security Configuration Status (Section 5.2.4)
6. Security Configurations, as required (Section 5.5)
7. Security Configuration Timer Table (Section 5.6)
8. PAC Size (Section 5.8.1)
9. Passenger Information (Section 5.7.3)
   a. Passenger Name
   b. Passenger Access Code
   c. Personal Time Schedule
   d. Group Assignment (Group Name)
   e. Floor Access (Floor Map)
10. Group Time Schedules, as required (Section 5.8)

SECTION 6
SECURITY INTERFACE SOFTWARE (SIS)

6.0 INTRODUCTION

MCE's elevator security options, Basic Security with CRT and Access Control for Elevators (ACE), are programmed using a CRT terminal or a PC. The **Security Interface Software (SIS)** is used to program the elevator security parameters using a PC.

The Security Interface Software can be run on the PC in the following ways:

- as a stand-alone DOS program
- launched from inside Windows
- launched from MCE's Central Monitoring System (CMS) for Windows software

The PC can be connected to the controller running the elevator security option:

- directly via serial cable
- via a serial cable plus line drivers (to extend the distance)
- via a phone line using a modem
- via an Ethernet connection through CMS

A block diagram of the components and cables to be used for the installation can be found on the *Peripherals Interface* page in the Job Prints for the job. MCE's Computer Peripherals Manual, part # 42-02-CP00, provides additional instructions including the proper jumper, switch and COM port settings.

ABOUT THIS SECTION - This section describes how to install and use the Security Interface Software. It is divided into the following sections:

Section 6.1, Getting Started - This section covers the system requirements and software installation. An overview of MCE's elevator security is also included.

Section 6.2, Security Job Connection Menu - This section covers the COM port and modem settings used to make the connection to the controller. If SIS will be accessed using MCE's Central Monitoring System (CMS) for Windows software, this section may be skipped.

Section 6.3, Security Interface Software Main Menu - The Main Menu for Access Control for Elevators (ACE) security has more options than the Main Menu for Standard Security. This section gives an indication of what can be accomplished using each menu option.

Section 6.4, Security Configuration Menu - This section pertains to both Standard and ACE Security. It explains how elevator security is turned ON or OFF using the various hardware and software settings. It covers programming the Security Configurations that set the security status for each floor. It also covers programming the Timer Table and how to activate a specific Security Configuration or select Timed to allow the current Security Configuration to be selected via the Security Configuration Timer Table.

Section 6.5, Passenger Information Menu - This section pertains only to ACE Security. It explains how to program the Passenger Data, including the Passenger Access Code (PAC), Floor Access Restrictions, Personal Timer Schedule and assigning a passenger to a Group.

Section 6.6, Report Generation Menu - A list of Secured Car Calls Registered is available with ACE Security. This section describes the options available in this menu.

Section 6.7, Change Controller Password - Access to the controller using the Security Interface Software can be password protected. This section describes how to set the password.

6.1 GETTING STARTED

6.1.1 SYSTEM REQUIREMENTS

To run the Security Interface Software, a computer system with at least the following is required:

✓ IBM compatible PC with:
- 1 MB RAM
- 40 MB hard disk
- 1 or more serial ports
- 1 3.5" floppy disk drive
- 1 VGA card

✓ 1 VGA monitor

✓ 1 Hayes compatible modem (if phone connection is used)

6.1.2 WINDOWS INSTALLATION

Use the following installation procedure to install the SIS program from Windows.

1. Insert the floppy disk containing the SIS program in drive **A:** or **B:**
2. Click on the **Start** button, then click on **Run**.
3. At the **Run** Command Line Entry, depending on the location of the floppy disk, Type **A:\SETUP**.
4. Follow the instructions on the screen to complete the installation.

6.1.3 CMS INSTALLATION

It is not necessary to install the Security Interface Software separately if SIS will be accessed using MCE's Central Monitoring System (CMS) for Windows software. The SIS program is installed when the CMS software is installed. Consult the Central Monitoring System (CMS) User's Guide, part # 42-02-S021, for installation instructions.

Note: When a Device Server is used, the ***security.ini*** file must be modified as follows:

1. Double-click **My Computer**, then double-click **C: drive** (or drive where CMS is installed).
2. Double-click **CMSWIN** folder.
3. Double-click the **security.ini** file to open it.
4. Under **[Security Call Lockout]**
   - for *Digi Port Server TS2*, set **Terminal=5**
   - for *CoBox-FL-01 Device Server*, set **Terminal=6**
5. Save and then close the **security.ini** file.

6.2 SECURITY JOB CONNECTION MENU

NOTE: If MCE's Central Monitoring System (CMS) for Windows software will be used to access the SIS program, skip this section and proceed to Section 3, *Security Interface Software Main Menu.*

If the SIS program is running as a stand alone DOS program or launched from Windows, the **SECURITY JOB CONNECTION MENU** is the first menu displayed. This menu allows setup of the communication parameters between the PC and the controller.

The current values of the communication parameters are displayed in the window just below the menu.

To select an option from the Security Job Connection menu, use the Up or Down **arrow** keys to highlight the desired option and then press **Enter** or press the letter that is highlighted in the menu option. For example, to select the option "**Specify Baud Rate**," either highlight it using the arrow keys and press **Enter** or press the letter "**B**" on the keyboard.

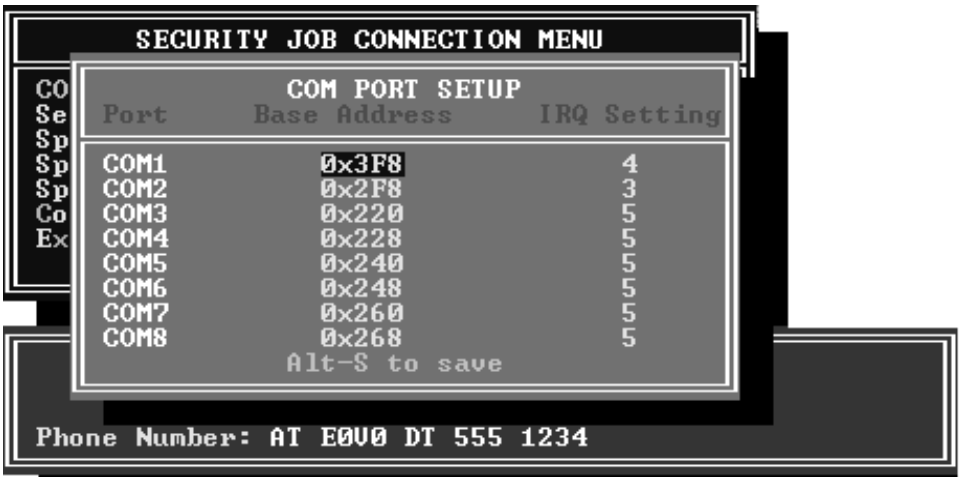
The menu options and their functions are described in detail in the following sub-sections.

6.2.1 COM PORT SETUP

This option is used to program the base address and IRQ setting for the PC's COM Ports. This option is used when more than two COM ports are used to access multiple controllers. The default settings for COM ports 1 and 2 are the normal PC default settings.

NOTE: Consult your Windows User's Manual to verify PC COM port resource settings before attempting any changes to the SIS COM Port setup.

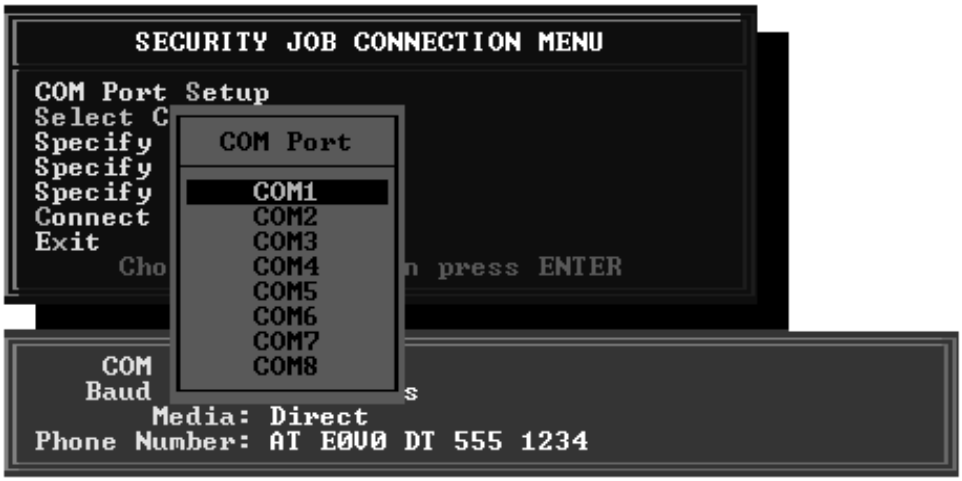
To select the COM Port Setup option use the **arrow** keys to highlight it and then press **Enter** or press the letter "**S**" on the keyboard. The following pop-up window displayed.



Use the **arrow** keys to highlight the item you wish to change and press the "**I**" or "**D**" key to increment or decrement the value. Press **Alt-S** to save the changes. Press **Esc** to return to the **Security Job Connection Menu**.

6.2.2 SELECT COM PORT

This option is used to select the Serial Port that to be use for communicating with the controller. To select this option use the **arrow** keys to highlight it and then press **Enter** or press the letter "**P**" on the keyboard.

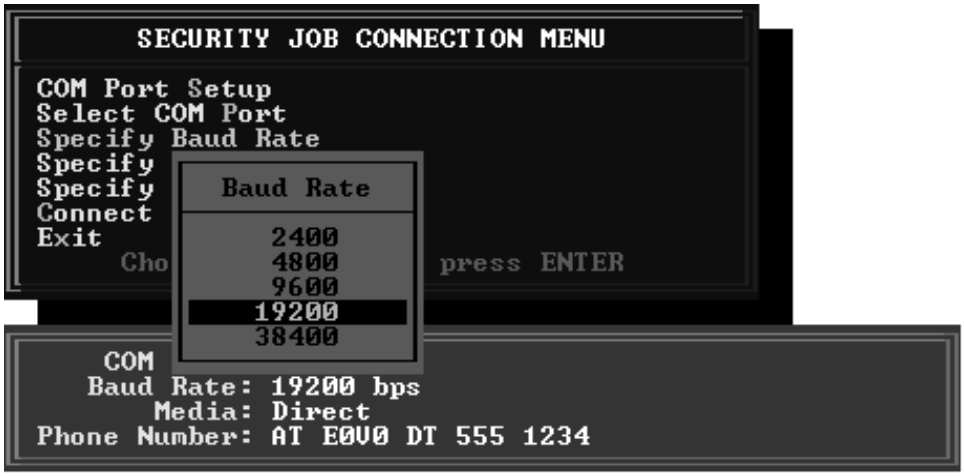


Once this option is selected, a pop-up window is displayed as shown above. Select the desired COM Port by highlighting it using the **arrow** keys and pressing **Enter**.

To cancel the operation and return to the **Security Job Connection Menu**, press the **Esc** key.

6.2.3 SPECIFY BAUD RATE

This option is used to select the communication baud rate between the PC and the controller. To choose this option, either highlight it using the **arrow** keys and press **Enter** or press the letter "**B**" on the keyboard.



Once selected, this option displays a pop-up window for choosing a Baud Rate as shown above. Use the **arrow** keys to choose a value for the Baud Rate and press **Enter**.

Select a baud rate that matches the baud rate of the communication media being used to connect to the controller. Refer to the baud rate information in the documentation provided by the communication media manufacturer. Then refer to the following table to select the proper baud rate for the communication media. To cancel the operation and return to the **Security Job Connection Menu**, press the **Esc** key.

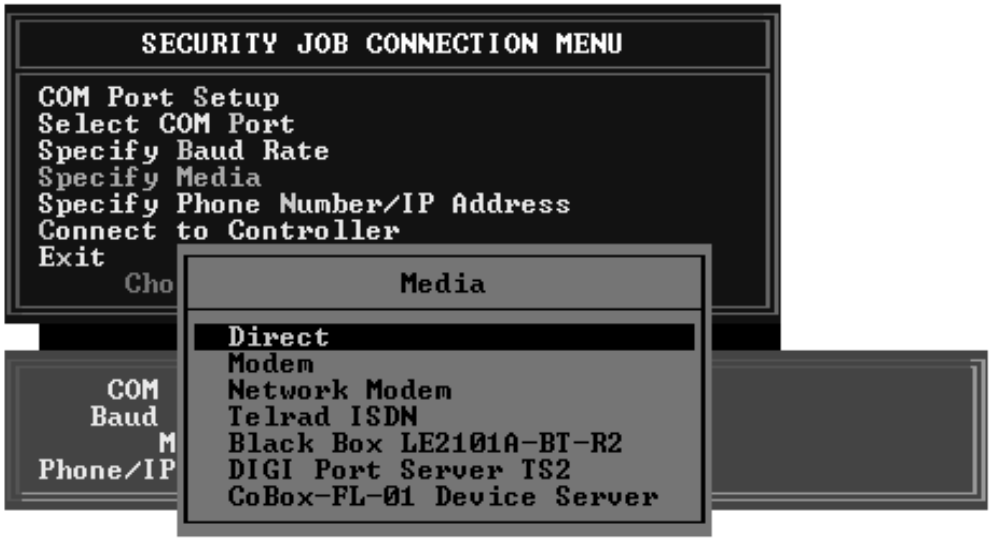
Communication Media	Baud Rate
Serial Cable *	19,200
Line Driver *	9600
Modem	modem specific, 2400 - 19,200
Network Modem	modem specific, 2400 - 19,200
Telrad ISDN	19,200
Black Box LE2101A-BT-R2	**
Digi Port Server TS 2	**
CoBox-FL-01 Device Server	**

* Note: For direct serial cable and line driver connections, select Direct Media.

** Note: COM port settings and baud rate are not used for Ethernet connection.

6.2.4 SPECIFY MEDIA

This option is used to select the communication Media between the PC and the controller. To choose this option, either highlight it using the **arrow** keys and press **Enter** or press the letter "**M**" on the keyboard.



Once selected, this option displays a pop-up window for choosing a Media as shown above. Use the **arrow** keys to choose a Media and press **Enter**. To cancel the operation and return to the **Security Job Connection Menu**, press the **Esc** key.

Specify Ethernet Connection - Three Ethernet device servers have been tested and proven compatible with this software. Select the option for the device server used:

- **Black Box LE2101A-BT-RT2** for Black Box LE2101A-BT-RT2 device server.
- **Digi Port Server TS 2** for Digi Port TS 2 device server.
- **CoBox-FL-01 Device Server** for LANTRONIX CoBox-FL-01 device server.

NOTE: For other device servers, call MCE Tech Support to determine compatibility with this software.

6.2.5 SPECIFY PHONE NUMBER / IP ADDRESS

If a modem or Ethernet connection will be used to communicate with the controller, use this option to specify the phone number or IP Address. To choose this option, either highlight it using the **arrow** keys and press **Enter** or press the letter "**N**" on the keyboard.

Once selected, this option displays a pop-up window listing the existing phone numbers / IP Addresses. Use the **arrow** keys to choose a (job) **Name** and press **Enter**.

To add a new phone number into the list, use the down arrow key to go to an empty line and enter the relevant information. Additional characters may be required depending on the modem to be used. Refer to the documentation provided by the modem manufacturer.

If device servers will be used to communicate with the controller, add a new IP Address and port Number. For Digi Port Server TS2 use the format **IP Address[space]port number**, for example (125.10.12.126 2001). For Lantronics CoBox-FL-01 use the format **IP Address[,]port number**, for example (125.10.12.126,2001). **Note the difference:** Digi uses a space and Lantronics uses a comma between the IP Address and the port number.

To cancel the operation and return to the **Security Job Connection Menu**, press the **Esc** key.

6.2.6 CONNECT TO CONTROLLER

After selecting the desired communication parameters, connection to the controller can be attempted. To connect to the controller, either choose this option using the **arrow** keys and press **Enter** or press the letter "**C**" on the keyboard.

When connected, the system will prompt for the password as shown above. Type in the password and press **Enter**. If no password has been programmed press **Enter** to gain access. Section 7 explains how to program the password.

LOST OR FORGOTTEN PASSWORD - If you don't remember the password, press "**?**" on the keyboard. This displays the Lost Password window.

Make a note of the Reference # and contact MCE Technical Support for a temporary password. Type in the temporary password and press **Enter**. If you make a mistake while typing the temporary password, try again. Choose a new password, type it in and press **Enter.** Then confirm the new password by typing it in again and pressing **Enter**.

After verification of the temporary password as well as the new password, the new password is uploaded to the controller. Use this new password at the Login prompt when you next log in.

6.2.7 Exit

To Exit the SIS program, select this option using the arrow keys and press **Enter** or press the letter "**X**" on the keyboard.

6.3 SECURITY INTERFACE SOFTWARE MAIN MENU

Once the connection to the controller has been established and the Login Password is verified, the system displays the **Security Interface Software Main Menu**.

The number of options in the Main Menu depends on the type of security running on the controller, Basic Security or Access Control for Elevators (ACE). With Basic Security the *Passenger Information Menu* and *Report Generation Menu* options will not be available.

6.3.1 BASIC SECURITY MAIN MENU

With MCE's Basic Security the following Main Menu is displayed.

To select an option, use the Up or Down **arrow** keys to highlight the desired option and then press **Enter** or press the key for the letter that is highlighted (displayed in a different color) in the menu option.

Security Configuration Menu - Select this menu to:

- program or modify a Security Configuration (see Section 6.4.2)
- program or modify the Security Configuration Timer Table (see Section 6.4.3)
- activate a Security Configuration (see Section 6.4.4)
- change the Security Software Switch setting (see Section 6.4.5)

Change Controller Password - Use this to change the Password (see Section 6.7)

Exit (Disconnect) - Use this to disconnect the connection to the controller.

6.3.2 ACCESS CONTROL FOR ELEVATORS (ACE) MAIN MENU

With Access Control for Elevators (ACE) security the following Main Menu is displayed.

To select an option, use the Up or Down **arrow** keys to highlight the desired option and then press **Enter** or press the key for the letter that is highlighted (displayed in a different color) in the menu option.

Security Configuration Menu - Select this menu to:

- program or modify a Security Configuration (see Section 6.4.2)
- program or modify the Security Configuration Timer Table (see Section 6.4.3)
- activate a Security Configuration (see Section 6.4.4)
- change the Security Software Switch setting (see Section 6.4.5)

Passenger Information Menu - Select this menu to:

- modify Passenger Data (see Section 6.5.1)
- modify Group Data (see Section 6.5.2)
- set the Length of Passenger Access Codes (see Section 6.5.3)

Change Controller Password - Use this to change the Password (see Section 6.7)

Exit (Disconnect) - Use this to disconnect the connection to the controller.

6.4 SECURITY CONFIGURATION MENU

To select this option from the Main Menu, use the **arrow** keys to highlight it, then press **Enter** or press the letter "**C**" on the keyboard. The following menu is displayed.

6.4.1 SECURITY STATUS - TURNING SECURITY ON AND OFF

The status of the elevator security parameters is displayed in a window below the menu. Four of these parameters, (1) Security Configuration Status, (2) Master Software Key, (3) Security Software Switch and (4) BSI, determine the overall Security Status. These parameters are described below and Table 6.1, *Security Status Decision Matrix,* describes their effect on the overall Security Status.

Security Status - This is the overall security status, ON or OFF.

Security Configuration Status - Shows the current Security Configuration and how it was activated, Manual or Timed.

Master Software Key - This is the MSK, Master Software Key parameter which is set using the Computer Swing Panel Enhanced On-Board Diagnostics (see Section 5 of the controller manual). Table 6.1 shows how the Master Software Key affects the overall Security Status.

Security Software Switch - The Security Software Switch can be set to ON or OFF using the **"**Modify the Security Software Switch**"** option in the Security Configuration Menu. Table 6.1 shows how the Security Software Switch affects the overall Security Status.

BSI - This is an optional controller input which can be connected to a hardware switch for activation. Table 6.1 shows how the BSI input affects the overall Security Status.

TABLE 6.1 Security Status Decision Matrix

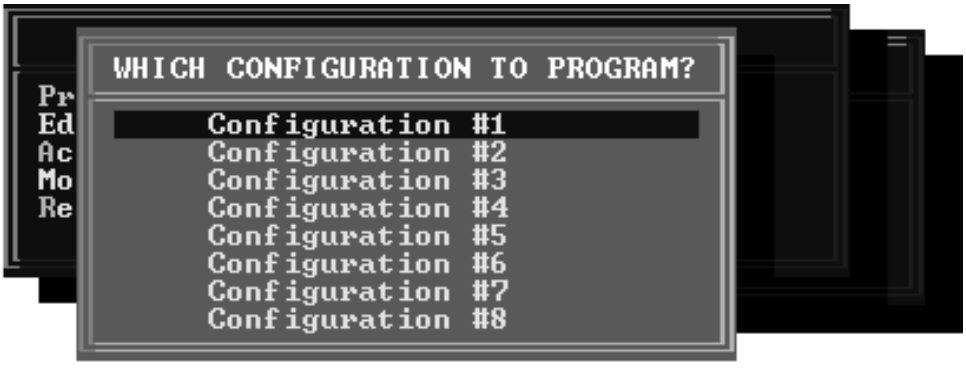
Inputs or Software Settings				Outputs or Results	
Master Software Key	**Security Software Switch**	**BSI✶ Input (optional)**	**Security Configuration**	**Security Configuration in use**	**Security Status**
Deactivated	n/a	n/a	n/a	none	**OFF**
Activated	n/a	n/a	n/a	1	**ON**
Enabled	ON	n/a	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table
	OFF	OFF	n/a	none	**OFF**
		ON	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table

✶ Ignore the shaded area unless the controller has the BSI input.

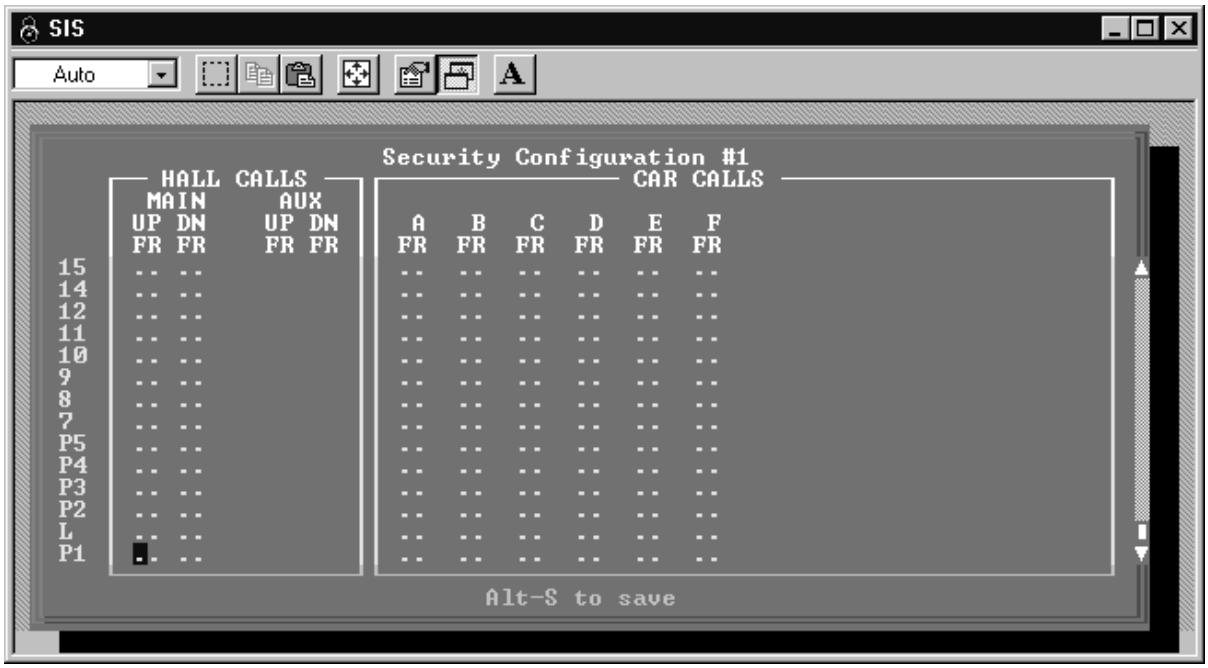
The various menu options and their functions are described in the following sub sections:

6.4.2 PROGRAM A SECURITY CONFIGURATION

This option is used to program 8 possible security configurations. These configurations may be selected and activated later using the **"Activate a Security Configuration"** option from the **Security Configuration Menu**. To select this option, use the **arrow** keys to highlight the option and press **Enter** or press the letter "**P**" on the keyboard. A pop-up window with a list of configurations as shown below is displayed.



Select the configuration to program using the **arrow** keys and press **Enter**. This opens another window as shown.



This window displays a column with all the floors in the building at the extreme left of the window. To the right of the floors is a box that contains the various **HALL CALLS**. There are two columns within this box. One for the main hall calls labeled **MAIN** and the other for the auxiliary hall calls labeled **AUX**. The labels **UP** and **DN** refer to the directions **up** and **down** respectively. The labels **F** and **R** refer to the **front** and **rear** doors respectively. The security status of hall calls can be set to *Locked* (**L**) or *Unsecured* (**.**). Section 1.5, *An Overview of MCE's Elevator Security* describes these settings.

The box on the right side of the window contains all the **CAR CALLS**. The columns for the various cars are labeled **A**, **B**, **C**, **D**... or 1, 2, 3, 4...and so on. The security status of car calls can be set to *Locked* (**L**), *Secured* (**S**) or *Unsecured* (**.**). Section 1.6, *An Overview of MCE's Elevator Security* describes these settings.

To change the security status of a particular hall call or car call, position the cursor on the desired field using the **arrow** keys. To change the status, use the letters "**D**" or "**I**" on the keyboard to scroll through the security choices or press the "**L**", "**S**" or "**.**" key. When finished, press **Alt-S** to save the configuration. Press the **Esc** key to return to the previous menu.

PER-CAR HALL CALL SECURITY - If so ordered from the factory, your system may offer Per Car Security. Programming Per Car Security is essentially the same, the difference being that each elevator car may be set to respond to hall calls independently.

NOTE: With ***Basic Security***, the Security Codes are programmed using each car controller's Main Computer. A floor cannot be *Secured* unless a Security Code has been programmed for that floor. Instructions for programming the Security Codes is found in Section 2.3,*Viewing and Changing the Security Codes - PTC and PHC* and in Section 2.4, *Viewing and Changing Security Codes - Swing Panel*.

6.4.3 EDIT THE SECURITY CONFIGURATION TIMER TABLE

To select this option, use the arrow keys to highlight the option and press **Enter** or press the letter "**B**" on the keyboard. A pop-up window with a list of Security Configuration Timers and their status is displayed.

SECURITY CONFIG. TIMER TABLE Status

Timer	Day	Begin	End	Config	(ON/OFF)
1	ALL	00:00	23:59	1	ON
2	ALL	00:00	23:59	1	OFF
3	ALL	00:00	23:59	1	OFF
4	ALL	00:00	23:59	1	OFF
5	ALL	00:00	23:59	1	OFF
6	ALL	00:00	23:59	1	OFF
7	ALL	00:00	23:59	1	OFF
8	ALL	00:00	23:59	1	OFF
9	ALL	00:00	23:59	1	OFF
10	ALL	00:00	23:59	1	OFF
11	ALL	00:00	23:59	1	OFF
12	ALL	00:00	23:59	1	OFF
13	ALL	00:00	23:59	1	OFF
14	ALL	00:00	23:59	1	OFF
15	ALL	00:00	23:59	1	OFF
16	ALL	00:00	23:59	1	OFF

Alt-S to save

This option is used to program the 16 time schedules, Timer #1 thru #16, which select the *current* Security Configuration when **Timed** is selected using the "*Activate a Configuration*" selection. Each timer specifies a **Day**, **Begin** time, **End** time, Configuration Number (**Config**) and timer **Status**. The timers are searched continuously to achieve automatic switching of configurations. The *Config* number in the highest priority timer with a *Status* of ON that is valid for this day and time (current time is between Begin and End time) determines the *current* Security Configuration. If no timers are valid, the Configuration status will be **Timed OFF** and the *Security Status* will be **OFF**.

Timer priority is determined by the timer number. Timer #1 has highest priority and Timer # 16 has lowest priority.

Use the **arrow** keys to select the field to change. Use the letters "**D**" or "**I**" on the keyboard to scroll through the values available for the selected field. Press **Alt-S** to save the configuration. Press **Esc** to return to the previous menu.

Day represents the day(s) of the week on which the selected configuration will be activated. The values for Day are MON, TUE, WED, THU, FRI, SAT, and SUN representing each day of the week respectively, M-F representing Monday through Friday and ALL meaning every day.

Begin is the time, in hours and minutes, when the selected configuration will be activated. **End** is the time, in hours and minutes, when the selected configuration will be deactivated. The earliest time is 00:00 and the latest time is 23:59. Both start time and end time must be in the same day. No time period can be defined greater than 24 hours or defined across midnight. Any timer with an end time of 23:59 will be automatically extended to midnight to avoid an undefined minute, 23:59 to midnight.

The configuration number, **Config**, can be any one of the eight Security Configurations described in Section 6.4.2.

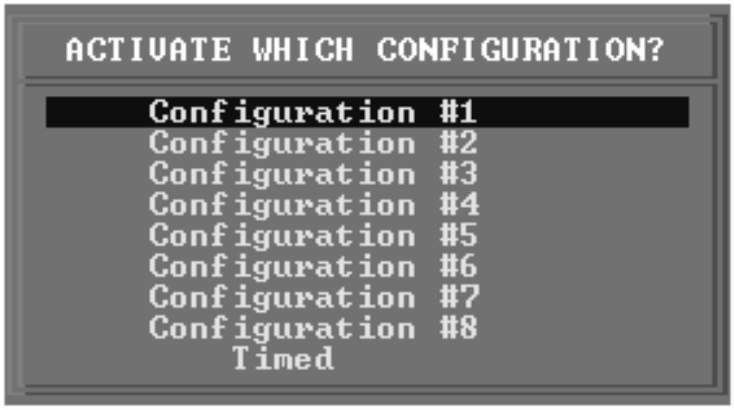
The Timer **Status** can be either ON or OFF. When the timer status is OFF, the timer settings are ignored.

CAUTION: Be careful not to define timers that overlap. If the *Start Time* of one timer is earlier than the *End Time* of another timer they may not operate as expected.

Example: Suppose you would like to use Security Configuration #5 overnight, from 20:00 (8 pm) to 6:00 (6 am) Monday through Friday. Use two timers and set the Day field of both timers to M-F. Set one timer's start time to 20:00 and end time to 23:59. Set the second timer's start time to 00:00, and End Time to 06:00. Set Config. # to 5 and Timer Status *ON* for both timers.

6.4.4 ACTIVATE A SECURITY CONFIGURATION

This option is used to activate a Security Configuration that has been programmed using the **"**Program a Security Configuration**"** option. To select this option, use the **arrow** keys to highlight the "Activate a Security Configuration" option and press **Enter** or press the letter "**A**" on the keyboard. The following pop-up window is displayed.



Select the desired configuration (Configuration #1 through #8) using the **arrow** keys and press **Enter** to activate it. If Configuration #4 is activated, the **Security Configuration Status** will be **Manual #4**. The selected configuration will remain active until changed.

If **Timed** is selected, then the currently selected configuration is determined by the settings in the Security Configuration Timer Table (refer to Section 6.4.2). If the Timer Table selects Configuration #6, the **Security Configuration Status** will be **Timed #6**. If no timers are valid, the **Security Configuration Status** will be **Timed OFF** and the Security Status will be OFF.

Press the **Esc** key to return to the previous menu.

6.4.5 MODIFY THE SECURITY SOFTWARE SWITCH

This option is used to change the settings of the Security Software Switch. To select this option, use the **arrow** keys to highlight the selection and press **Enter** or press the letter "**W**" on the keyboard. The following pop-up window is displayed.

Select the desired setting, ON or OFF using the **arrow** keys and press **Enter**. Refer to Table 6.1, *Security Status Decision Matrix*, for a description of how the Security Software Switch affects the overall Security Status.

Press the **Esc** key to return to the previous menu.

6.4.6 RETURN TO MAIN MENU

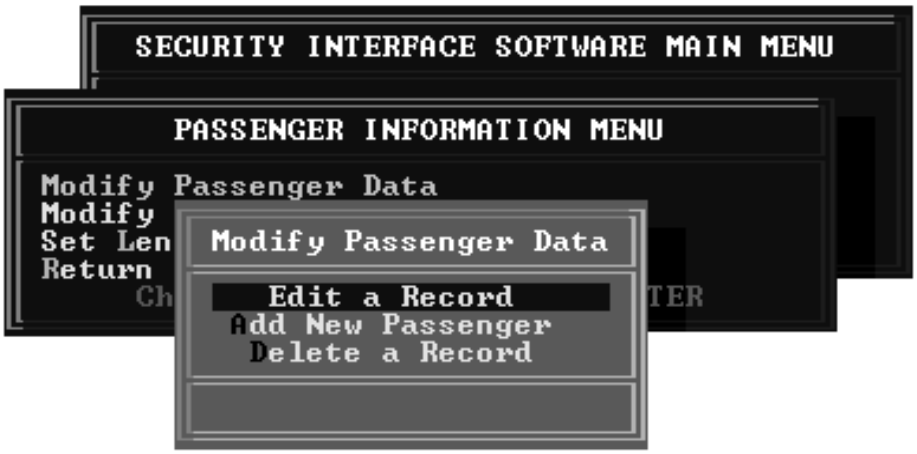
Press the **Esc** key or the letter "**R**" on the keyboard to return to the Security Interface Software Main Menu.

6.5 PASSENGER INFORMATION MENU

This option is only available for controllers with Access Control for Elevators (ACE) security. To select this option, choose it using the **arrow** keys and press **Enter** or press the letter "**P**" on the keyboard. When selected, this option displays a sub menu as shown below.

6.5.1 MODIFY PASSENGER DATA

This option allows modification of the passenger information on the controller. To select this option, highlight it using the **arrow** keys and press **Enter** or press the letter "**P**" on the keyboard. When selected, it displays the pop-up menu shown below.



The various menu options and their functions are described in the following sub sections:

6.5.1.1 EDIT A RECORD - This option is used to edit the information for an existing passenger. To select this option, choose it using the **arrow** keys and press **Enter** or press the letter "**E**" on the keyboard. When selected, it displays a list of existing passengers sorted alphabetically based on their first names.

Select the desired passenger using the **arrow** keys and press **Enter** to display a menu for that passenger as shown in the following.

The various menu options and their functions are described in the following sub sections:

CHANGE PASSENGER'S NAME - This option is used to change the selected Passenger's Name. To select this option, highlight it using the **arrow** keys and press **Enter** or press the letter "**N**" on the keyboard. This displays a pop-up window as shown.

Make the desired changes in the Passenger's Name and press **Alt-S** to save it. Press the **Esc** key to return to the previous menu.

CHANGE PASSENGER'S ACCESS CODE - This option is used to change the selected passenger's access code. To select this option, highlight it using the arrow keys and press **Enter** or press the letter "**C**" on the keyboard. This displays a pop-up window as shown.

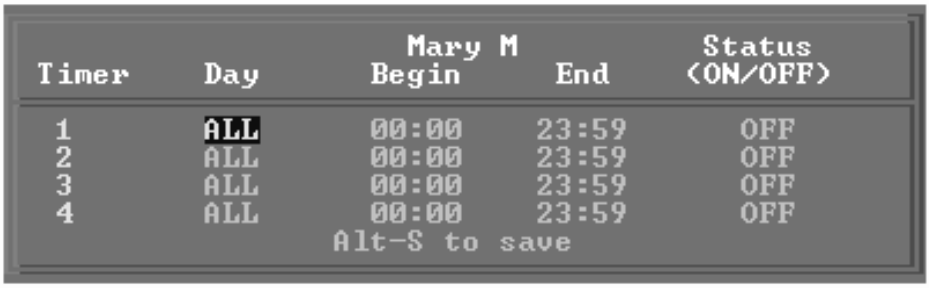
Use the **arrow** keys to position the cursor on the desired code. Use the letters "**I**" or "**D**" on the keyboard to scroll through the choices available. When the desired changes have been made, press **Alt-S** to save it. Press the **Esc** key to return to the previous menu.

ENTER FLOOR ACCESS RESTRICTIONS - This option is used to set the floor access restrictions for the selected passenger. To select this option, highlight it using the **arrow** keys and press **Enter** or press the letter "**R**" on the keyboard. This displays a pop-up window as shown below.

Use the **arrow** keys to position the cursor on the desired field. Use the letters "**I**" or "**D**" on the keyboard to make the desired changes in the Passenger's Floor Access Restrictions and press **Alt-S** to save it. Press the **Esc** key to return to the previous menu.

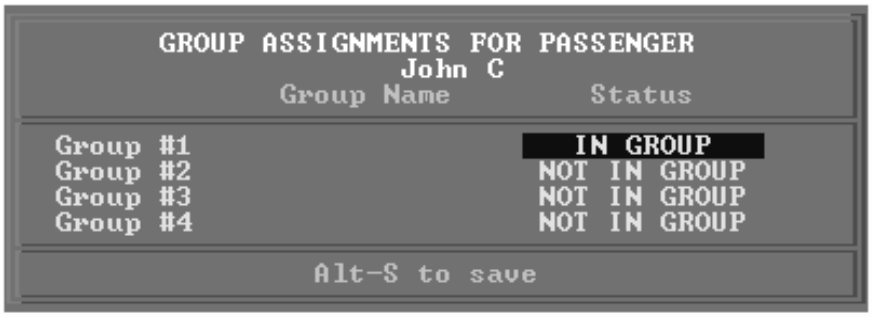
EDIT PERSONAL TIMER SCHEDULE - This option is used to edit the selected passenger's personal timer schedule. The purpose of the personal timer schedule is to determine the times that the selected passenger can access the elevator. This allows the building manager the flexibility to provide a passenger with access to the elevator during off hours and/or weekends.

To select this option, highlight it using the **arrow** keys and press **Enter** or press the letter "**T**" on the keyboard. This displays a pop-up window as shown below.



Use the **arrow** keys to position the cursor on the desired status field. Use the letters "**I**" or "**D**" on the keyboard to make the desired changes in the Passenger's Personal Timer Schedule and press **Alt-S** to save it. Press the **Esc** key to return to the previous menu.

ASSIGN PASSENGER TO A GROUP - This option is used to assign the selected passenger to one or more groups. There are 4 groups that can be used for assignments. This gives the building manager the flexibility to change the group's active time instead of changing the personal timer table for each passenger. To select this option, highlight it using the **arrow** keys and press **Enter** or press the letter "**G**" on the keyboard. This displays a pop-up window as shown.



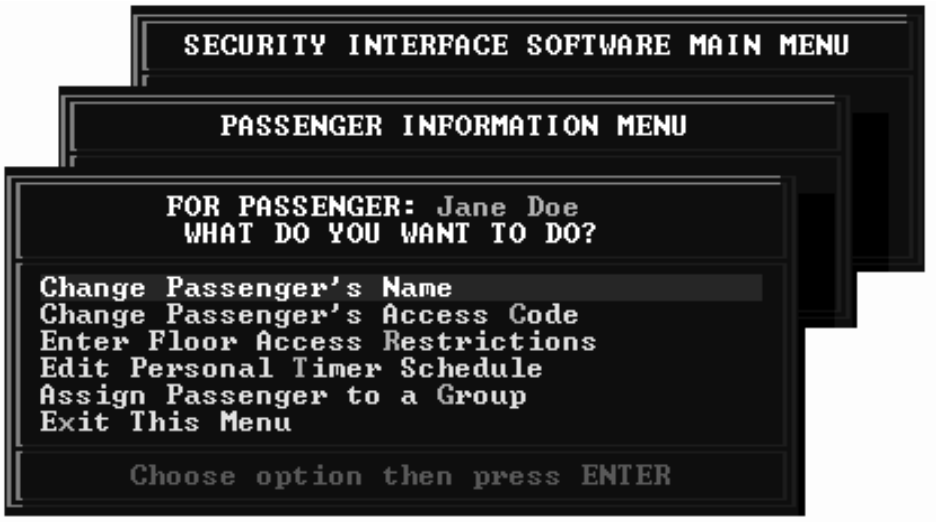
Use the **arrow** keys to position the cursor on the desired status field. Use the letters "**I**" or "**D**" on the keyboard to make the desired changes in the Group Assignments For Passenger window and press **Alt-S** to save it. Press the **Esc** key to return to the previous menu.

EXIT THIS MENU - Choose this option using the **arrow** keys and press **Enter** or either press the letter "**X**" or the **Esc** key on the keyboard to return to the previous menu.

6.5.1.2 ADD NEW PASSENGER - This option is used to add a new passenger to the existing list of passengers. To select this option from the "**Modify Passenger Data**" menu, highlight it using the **arrow** keys and press **Enter** or press the letter "**A**" on the keyboard. This displays a pop-up window as shown below.

Replace **<new passenger>** with the name of the desired new passenger. Press **Alt-S** to save the record. Press the **Esc** key to return to the previous menu.

After the new record is saved the menu below is displayed. This menu is the same as the "Edit a Record" menu. Refer to Section 6.5.1.1 for a detailed description of the menu items and functions.

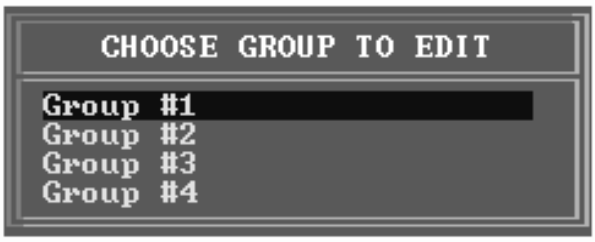


6.5.1.3 DELETE A RECORD - This option is used to permanently remove a passenger from the passenger list. To select this option from the "**Modify Passenger Data**" menu, highlight it using the arrow keys and press **Enter** or press the letter "**D**" on the keyboard. This displays a pop-up window with a list of all passenger names as shown below.

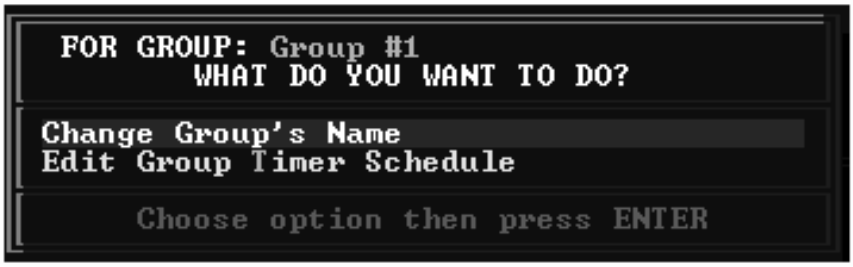
To mark a name for deleting, use the **arrow** keys to select the name then press "**D**". To Undelete a name use the arrow keys to select the name then press "**U**". Press **Alt-S** to save the record. Press the **Esc** key to return to the previous menu.

6.5.2 MODIFY GROUP DATA

This option is used to modify the group data. Choose the option from the **"Passenger Information Menu**" using the **arrow** keys and press **Enter** or press the letter "**G**" on the keyboard to activate this option. Once this option is activated, a pop-up list is displayed as shown below.



Choose a Group using the **arrow** keys and press **Enter** to modify it. This action displays a menu as shown.



The various menu options and their functions are described in the following sub sections:

6.5.2.1 CHANGE GROUP'S NAME - This option is used to change the name of the selected group. Choose the option using the **arrow** keys and press **Enter** to select it or press the letter "**N**" on the keyboard. A pop-up screen as shown bellow is displayed.

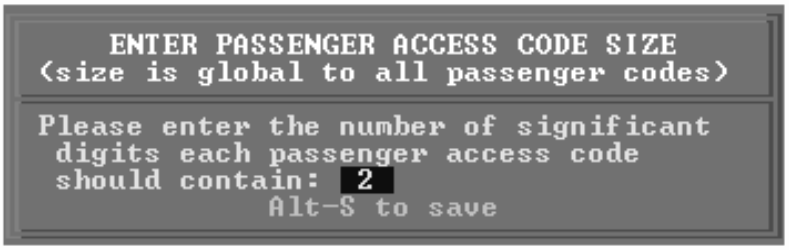
Make the desired changes in the group's name and press **Alt-S** to save the changes. Press the **Esc** key to return to the previous menu.

6.5.2.2 EDIT GROUP TIMER SCHEDULE - This option is used to edit the selected group's timer schedule. Choose the option using the **arrow** keys and press **Enter** to select it or press the letter "**T**" on the keyboard. A pop-up screen as shown below is displayed.

Use the **arrow** keys to position the cursor on the desired field. Use the letters "**I**" or "**D**" on the keyboard to make the desired changes in the Group's Timer Table and press **Alt-S** to save it. Press the **Esc** key to return to the previous menu. For more information refer to Section 6.4.3, *Edit the Security Configuration Timer Table.*

6.5.3 SET LENGTH OF ACCESS CODES

This option is used to set the size of the Passenger Access Code (PAC). Choose the option using the **arrow** keys and press **Enter** to select it or press the letter "**L**" on the keyboard. A pop-up screen as shown below is displayed.



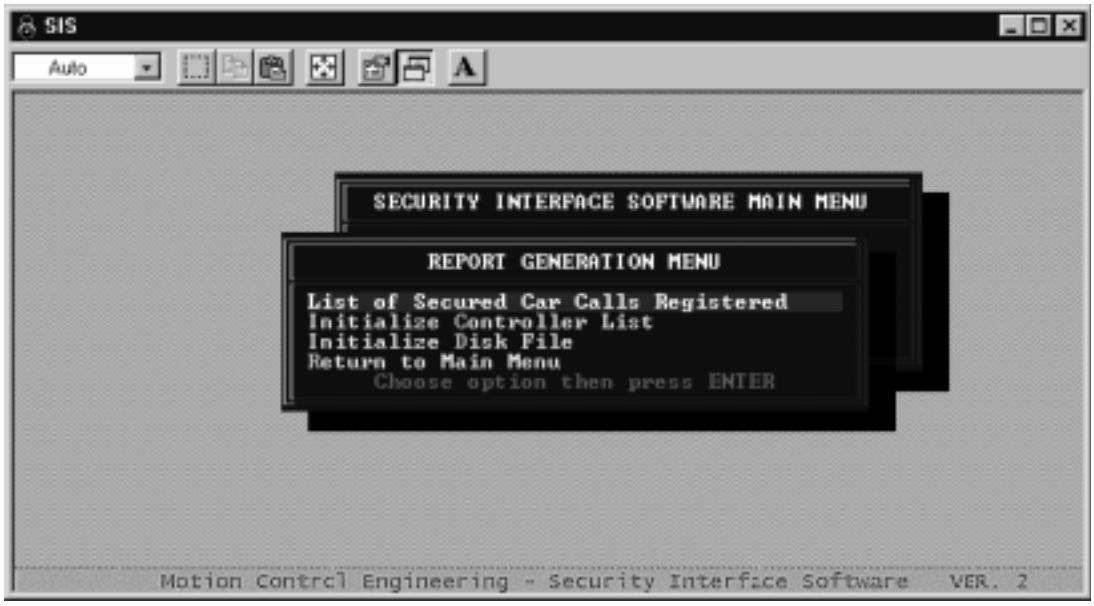
Use the letters "**I**" or "**D**" on the keyboard to make the desired changes in the size of the Passenger Access Code and press **Alt-S** to save it. Press the **Esc** key to return to the previous menu.

6.5.4 RETURN TO MAIN MENU

Choose this option using the arrow keys and press **Enter** or press the **Esc** key to return to the main menu.

6.6 REPORT GENERATION MENU

This option is only available for controllers with Access Control for Elevators (ACE) security. To select this option from the Main Menu, use the **arrow** keys to highlight the selection and press **Enter** or press the letter "**R**" on the keyboard. A sub menu as shown below is displayed.



6.6.1 LIST OF SECURED CAR CALLS REGISTERED

This option displays a list of secured car calls registered. To display this report, use the **arrow** keys to select the option and press **Enter** or press the letter "**S**" on the keyboard.

To print this report to a file on the computer, press **Alt-P**. The file will be saved as a ".txt" file in the folder (directory) in which the SIS program is located. The file name will be the job number plus ".txt" as shown on the report screen (98-1583.txt in this example). Each time the report is printed to file it is saved using this same file name. The previous file is overwritten. A text editor, such as Microsoft WordPad which comes with Window 95, can be used to print the report to a printer. Press the **Esc** key to return to the Report Generation Menu.

6.6.2 INITIALIZE CONTROLLER LIST

This option is used to delete all records and initialize the list of all car calls on the controller side. To activate this option, select it using the **arrow** keys and press **Enter** or press the letter "**C**" on the keyboard.

6.6.3 INITIALIZE DISK FILE

This option is used to delete all records and initialize the list of all car calls on the PC side. To activate this option, select it using the **arrow** keys and press **Enter** or press the letter "**D**" on the keyboard.

6.6.4 RETURN TO MAIN MENU

To return to the SIS Main Menu, select this option using the **arrow** keys and press **Enter** or press either the **Esc** key or the letter "**R**" on the keyboard.

6.7 CHANGE CONTROLLER PASSWORD

Use this option to change the Login password on the controller. Select the option using the arrow keys and press **Enter** or press the letter "**W**". A pop-up window as shown below is displayed.

- Enter the old password used to log on to the system and press **Enter**. This is used to verify that the person changing the password has access to the system.

- Enter the desired new password and press **Enter**.

- Re-enter the new password and press **Enter**. This is used to verify that the system has received the correct password.

After verification of the old as well as new passwords, the new password is uploaded to the controller. Enter this new password at the Login prompt.

SECTION 7
SECURITY INTERFACE SOFTWARE FOR WINDOWS

7.0 INTRODUCTION

Security Interface Software (SIS) for Windows is a Windows-native utility that allows you to administer MCE Basic or Access Control for Elevators (ACE) security systems. The software may be run independently or from the MCE Central Monitoring System (CMS) for Windows.

The PC may be connected to the controller running the elevator security option:

- Directly via serial cable
- Via a serial cable and line drivers (if necessary for long cable runs)
- Via a phone line/modem
- Via Ethernet connection

A block diagram of the components and cables used for installation is on the *Peripherals Interface* page of the Job Prints.

ABOUT THIS SECTION —- This section describes installing and using Security Interface Software for Windows, including:

Section 7.1 Getting Started —- System requirements and software installation.

Section 7.2 Connection Choices —- Select type of connection, COM port, and modem settings. If SIS will be accessed via Ethernet, this section may be skipped.

Section 7.3 Controller Menu —- You configure both Basic and ACE security systems through the Controller menu, including:

- Connecting/Disconnecting from the Controller
- Displaying Security Status
- Selecting a Controller Password
- Editing Security Configurations
- Editing Timer Tables
- Setting Configuration Status
- Setting the Security Software Switch
- ACE: Entering Passenger Data
- ACE: Entering Group Data
- ACE: Setting Access Code Length
- ACE: Generating Security Reports

Section 7.4 Help Menu —- Access to online help and software version information.

7.1 GETTING STARTED

This section describes:

- System requirements
- Software installation
- Startup

7.1.1 SYSTEM REQUIREMENTS

To run Security Interface Software for Windows, a computer system with at least the following is required:

✓ PC with Windows 98, 2000, or XP
✓ VGA monitor
✓ Hayes compatible 14.4k or higher baud modem (if phone connection is used)

7.1.2 STAND ALONE INSTALLATION

If you are installing MCE Central Monitoring System software, SIS for Windows will be included in that installation. (Refer to the Central Monitoring System User Guide, part # 42-02-S021 for appropriate instructions.) To install SIS for Windows alone:

1. Insert the SIS for Windows CD-ROM into your CD-ROM drive.
2. Access the disc and double-click the Setup.exe installer icon.
3. Follow the on-screen instructions.

7.1.3 STARTUP

To start the application, double-click the SIS for Windows program.

If you are accessing the elevator controller via Ethernet connection, go to Section **7.3 Controller Menu** and begin configuring the security system. If you are using any other means of connection, go to Section **7.2 Connection Choices** and configure your communications link first.

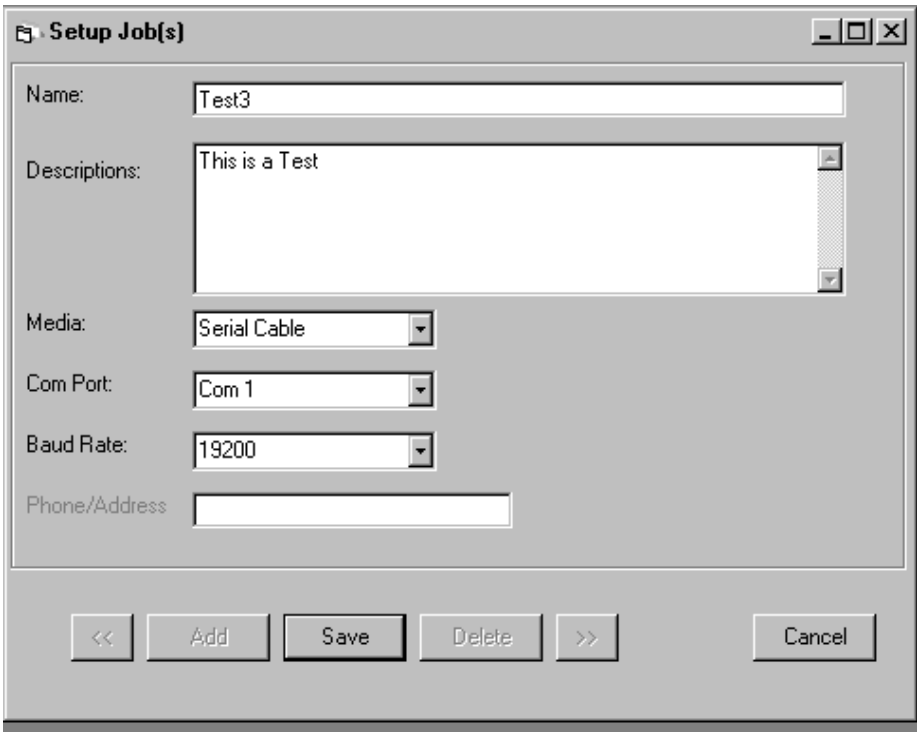
7.2 CONNECTION CHOICES

NOTE: If Ethernet will be used to access the controller, skip this section and proceed to Section 7.3 Controller Menu.

If you are connecting to the elevator controller other than through the MCE Central Monitoring System, you need to set up your connection to the controller before you can configure security. With SIS for Windows open, you will see the application menu bar.

To set up a connection:

1. Select **Job Configuration** under the **File** menu to open the setup dialog.



2. Enter a name in the Name: field for the connection you are creating. Once set up, you connect to a controller by selecting the connection name.
3. Provide a description of the connection so that its intended use will be clear to other users who might later edit the connection.
4. Select the connection method in the **Media:** drop-down menu. Choices are:
   - Serial Cable: Direct connection from a Com Port to the controller.
   - Line Driver: Connection via serial cable through a line driver.
   - Modem: Connection through a modem/phone line. See 7.2.1 Modem Configuration.
   - Digi Port Server TS2: Connection through a Digi Port TS2 device server.
   - CoBox-FL-01 Device: Connection through a CoBox-FL-01 device server.
5. Select the serial port that will be used to communicate with the controller.
6. Select a baud rate appropriate to the communications media selection. Refer to the following table.

Communication Media	Baud Rate
Serial Cable	19,200
Line Driver	9600
Modem	modem specific, 14,400 - 38,400
Digi Port Server TS 2	See Note
CoBox-FL-01 Device Server	See Note

* Note: COM port settings and baud rate are not used for Ethernet connection.

A device server is a hardware component that allows a PC to connect to Ethernet through a serial port. Two Ethernet device servers have been tested and proven compatible with this software:

- **Digi Port Server TS 2** for Digi Port TS 2 device server.
- **CoBox-FL-01 Device Server** for LANTRONIX CoBox-FL-01 device server.

Device servers must be properly installed. Refer to MCE setup instructions for Lantronix and Digi Port device servers, #42-IS-0058 and #42-IS-0060 respectively.

7. Specify a phone number if you are connecting via modem, or an IP Address if connecting through a device server. Some modem connections use special characters in the phone number. If you are not sure about your modem requirements, consult the modem manual.

DIGI Port and CoBox device servers use a specific IP Address/Port entry format:

- DIGI Port Server TS2: IP Address (space) port number. i.e., 125.10.12.126 2001.
- Lantronix CoBox-FL-01: IP Address (,) port number. i.e., 125.10.12.126,2001.

Note the difference: Digi uses a space where Lantronix uses a comma between the IP Address and the port number.

8. Once you have completed a job setup, click the Save button to save the configuration. When you use the connection in the future, you need only select **Connect** from the **Controller** menu and then select the job setup by its assigned name.

7.2.1 MODEM CONFIGURATION

If you are connecting via modem, you may also need to set modem type or special character requirements.

1. Select *Modem Configuration* from the *File* menu.
2. Set Modem Type and any special character requirements (Modem String).
3. Click Save.

7.2.2 ADD OR DELETE JOB SETUPS

From the Set Up Job(s) dialog, you may add a new Job Setup or delete an existing one.

To add a new Job Setup:

1. Select *Job Configuration* from the *File* menu.
2. Click *Add* to blank the entry fields in preparation for new entry.
3. Enter the new Job name.
4. Provide remaining Job information as described under 7.2 Connection Choices.
5. Click OK.

To delete an existing Job Setup:

1. Select *Job Configuration* from the *File* menu.
2. Use the left or right arrow keys to cycle through the Job Setups.
3. With the desired setup selected, click *Delete*.
4. Verify that you wish to delete the file.
5. Click *Save*.

7.3 CONTROLLER MENU

The Controller menu provides access to all security configuration options for Basic and ACE security systems.

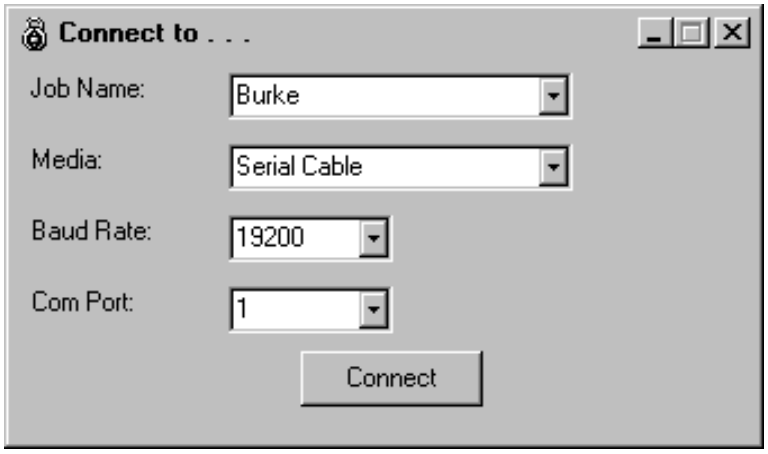
This section describes configuration for both options, including:

- 7.3.1 Connecting to a controller
- 7.3.2 Displaying security status
- 7.3.3 Selecting a controller password
- 7.3.4 Editing security configurations
- 7.3.5 Editing timer tables
- 7.3.6 Setting configuration status
- 7.3.7 Setting the Security Software Switch
- 7.3.8 Entering passenger data (ACE only)
- 7.3.9 Report Generation (ACE only)
- 7.3.10 Disconnecting from a controller

7.3.1 CONNECTING TO A CONTROLLER

To connect to a controller:

1. Select **Connect** from the **Controller** menu to display the connection dialog.



2. Select the desired Job Name (Burke in our example).

When you select the Job Name, Com Port, Baud Rate, Media, and Phone/Address (if used) information selected for that job will appear in the appropriate fields. If desired, you may select different criteria in these fields for **this** connection. (To change the information permanently, edit it in the Job Setup for the connection.)

3. Click on Connect. Connection progress dialogs will appear, followed by a password entry dialog.

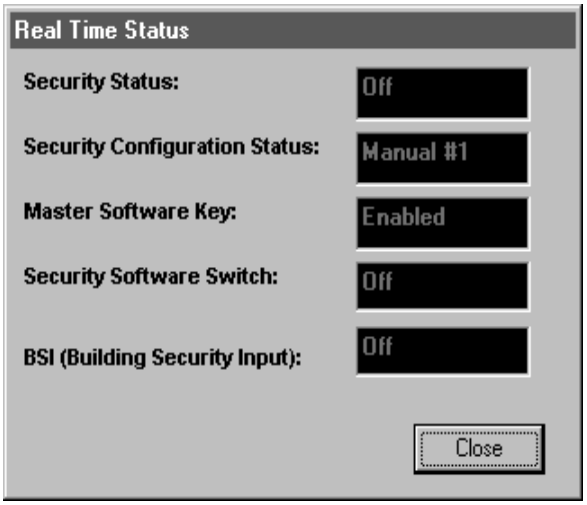
4. Enter the password, then click OK. For the initial logon, before a password has been programmed, simply click on OK without making an entry in the password field.

LOST OR FORGOTTEN PASSWORD - If you don't remember the password, press "?" on the keyboard (while the password entry dialog is displayed) to display the Lost Password window. Make a note of the Reference # and contact MCE Technical Support for a temporary password. Type in the temporary password and click OK.

You may change the connection password after successfully connecting to a controller. Refer to **7.3.3 Selecting a Controller Password** in this section.

7.3.2 DISPLAYING SECURITY STATUS

The security Real Time Status display provides an instant overview of system security status.



Security Status: Overall security status. On/Off.

Security Configuration Status: Displays the currently active security Configuration and whether it was activated manually (Manual) or automatically (Timed).

Master Software Key: Set from the controller Swing Panel as a function of Enhanced On-Board Diagnostics, the Master Software Key provides a failsafe method of enabling the security system when a terminal or PC is not available. For instructions on setting the Master Software Key, refer to the section of this guide (Sections 2 through 6) pertaining to your security installation.

The key may be Deactivated, Activated, or Enabled.

- When the Master Software Key is Deactivated, security is OFF.
- When the Master Software Key is Activated, security is ON with Configuration #1 active.
- When the Master Software Key is Enabled, security settings, and the status of the optional Building Security Input, determine the Configuration (#1 through #8) in use and whether or not security is currently ON or OFF. Refer to Table 7.1 for more information.

Security Software Switch: The Security Software Switch may be set to On or Off using the *Set Security Software Switch* function from the *Controller* menu. When set to ON, the security system determines whether security is active or inactive according to the selected security Configuration. Refer to Table 7.1 for more information.

BSI (Building Security Input): The Building Security Input is an optional controller input that may be connected to a hardware switch used to enable or disable security. Refer to Table 7.1 for more information.

TABLE 7.1 Security Status Decision Matrix

Inputs or Software Settings				Outputs or Results	
Master Software Key	**Security Software Switch**	**BSI✶ Input (optional)**	**Security Configuration**	**Security Configuration in use**	**Security Status**
Deactivated	n/a	n/a	n/a	none	**OFF**
Activated	n/a	n/a	n/a	1	**ON**
Enabled	ON	n/a	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table
	OFF	OFF	n/a	none	**OFF**
		ON	Manual 1 thru 8	1 thru 8 per Security Config. Status	**ON**
			Timed	1 thru 8 per Timer Table	**ON or OFF** per Timer Table

✶ Ignore the shaded area unless the controller has the BSI input.

7.3.3 SELECTING A CONTROLLER PASSWORD

The password used to connect to a controller may be changed if desired. To create or change a password (when currently connected to the controller):

1. Select *Change Controller Password* from the *Controller* menu to display the change password dialog.

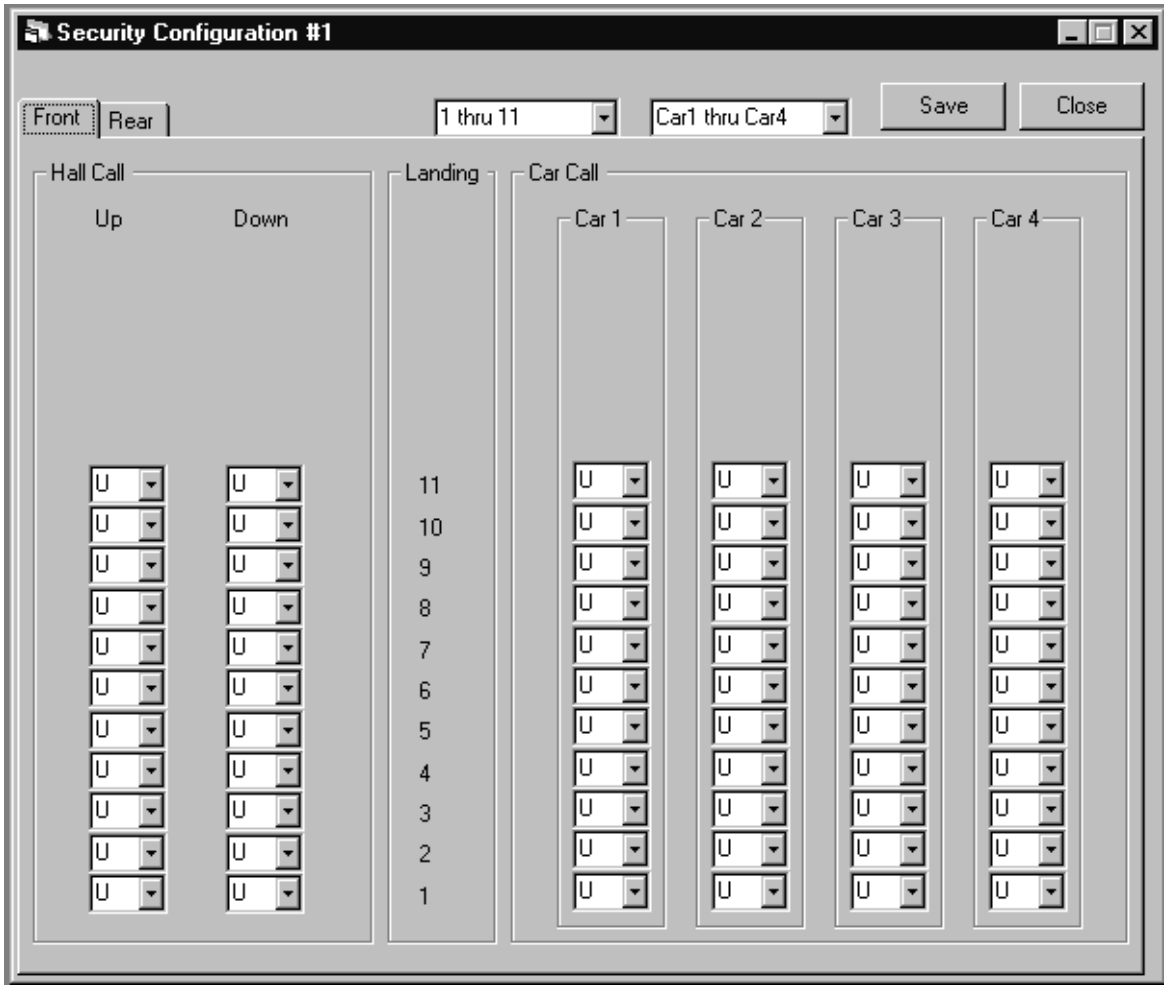
2. Enter the current password. (This ensures that the person changing the password has access to the system.)
3. Enter the new password.
4. In the final field, enter the new password a second time. (This is used to verify that the first entry was as intended.)
5. Click **Save.**

7.3.4 EDITING SECURITY CONFIGURATIONS

You may configure up to eight Security Configurations. Each Configuration allows you to selectively determine the security behavior of all hall call and car call panels for every elevator and every floor in your building. Using a configuration timer table, you may then selectively choose to automatically switch between programmed Security Configurations using one or more of sixteen timer schedules (Section 7.3.5). Depending upon how the controller was configured at the factory, your installation may use “standard” or “per car” security configuration.

To program a standard Security Configuration:

1. Select *Edit Security Configuration*/*Configuration #1 —- #8* from the *Controller* menu to open a programming dialog for the selected Configuration.



2. Select the floor and car ranges to be displayed.

Security selections within the dialog relate to the floor/landing with which they are horizontally aligned. In the sample dialog shown above, Hall Call and Car Call security can be selectively set for landings 1 through 11 respectively.

To set security for a particular landing, for the car group displayed:

3. For the landing hall calls, select whether the hall calls displayed are associated with the front or rear elevator doors by clicking on either the Front or the Rear control tab respectively. (This may not pertain in all situations.)

4. Set the hall calls for Up and Down directions independently:
   - U: Unsecured – Normal, unrestricted operation.
   - L: Locked – No access. The hall call will not be registered.

5. Set the car calls for each elevator independently for access to the associated floor.
   - U: Unsecured – Normal, unrestricted operation.
   - L: Locked – No access. The car call will not be registered for access to this floor.
   - S: Secured – Restricted access. The car will access the selected floor only if a valid security code is entered into the car control panel (and, for ACE systems, during a period of time for which the individual or group timer allows that code access.)

NOTE: For Basic and Basic with CRT security systems, a floor cannot be secured unless a security code has been programmed into the individual Car Controller's Main Computer. Refer to Viewing and Changing the Security Code in Section 2 (Basic) or Section 3 (Basic with CRT) respectively.

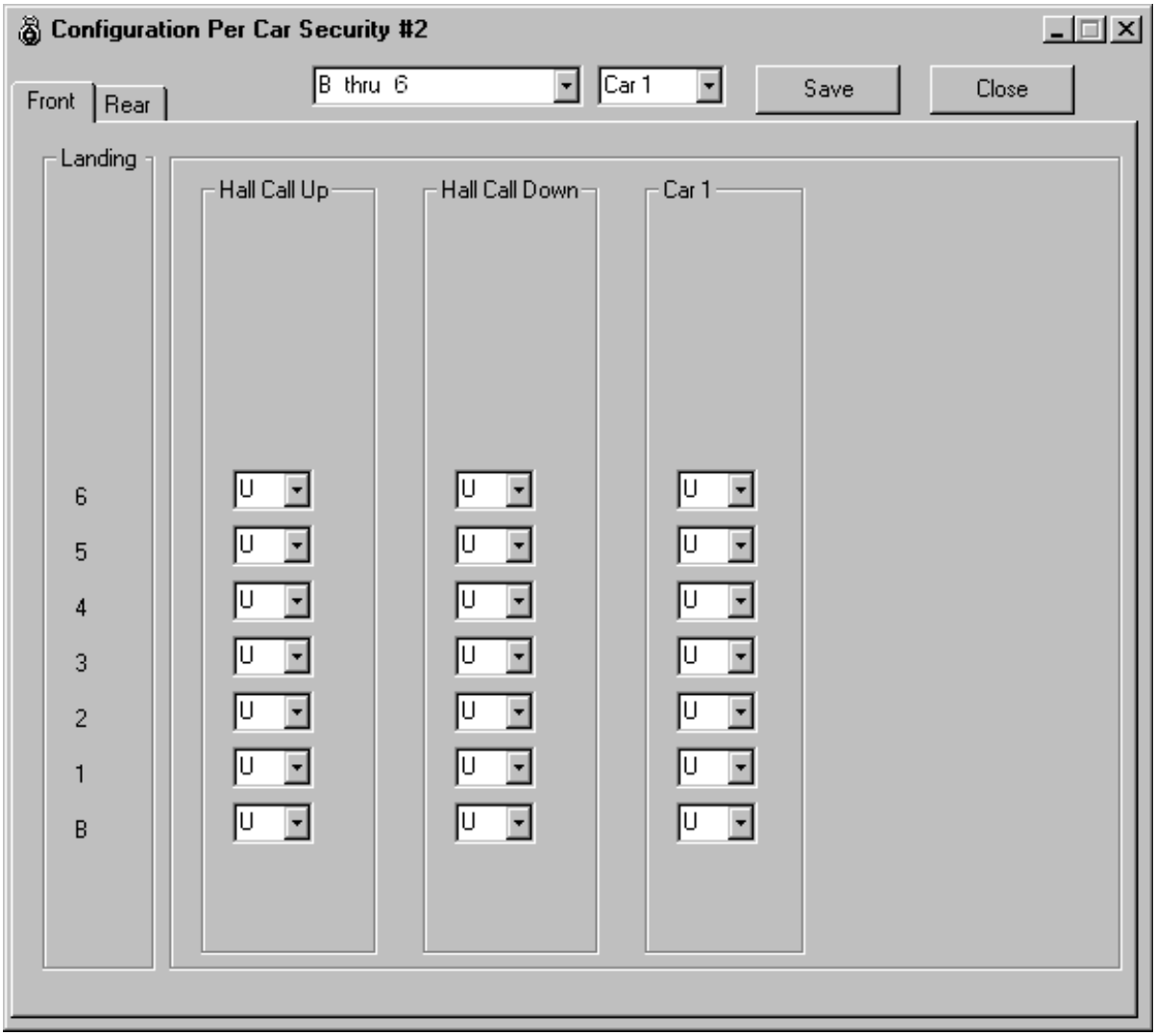
Floors for which a security code and a Security Configuration have been programmed are *secured* when that configuration is active and security is ON. In order to gain access to a secured floor via the elevator, the correct security code must be entered using the Car Operating Panel. When a car button for a secured floor is pressed, the button indicator will flash to indicate that a valid security code must be entered within ten seconds. If not, the call will not be registered.

6. Click **Save** to save changes to the Security Configuration or click **Close** before clicking Save to leave the dialog without accepting any unsaved changes.

To program a per car Security Configuration:

The per car configuration allows you to selectively determine which car or cars will respond to up and/or down hall calls (front and/or rear door) on a particular landing.

1. Select *Edit Security Configuration*/*Configuration #1 —- #8* from the *Controller* menu to open a programming dialog for the selected Configuration.



2. Select the floor range to be displayed.
3. Select the car to be configured for the selected floors.

Security selections within the dialog relate to the floor/landing with which they are horizontally aligned. In the sample dialog shown above, Hall Call and Car Call security can be selectively set for Car 1, landings B through 6 respectively.

To set security for a particular landing, for the car selected:

4. For the landing hall calls, select whether the hall calls displayed are associated with the front or rear elevator doors by clicking on either the Front or the Rear control tab respectively. (This may not pertain in all situations.)

5. Set the hall calls for Up and Down directions independently:
   - U: Unsecured – Normal, unrestricted operation.
   - L: Locked – No access. The hall call will not be registered.

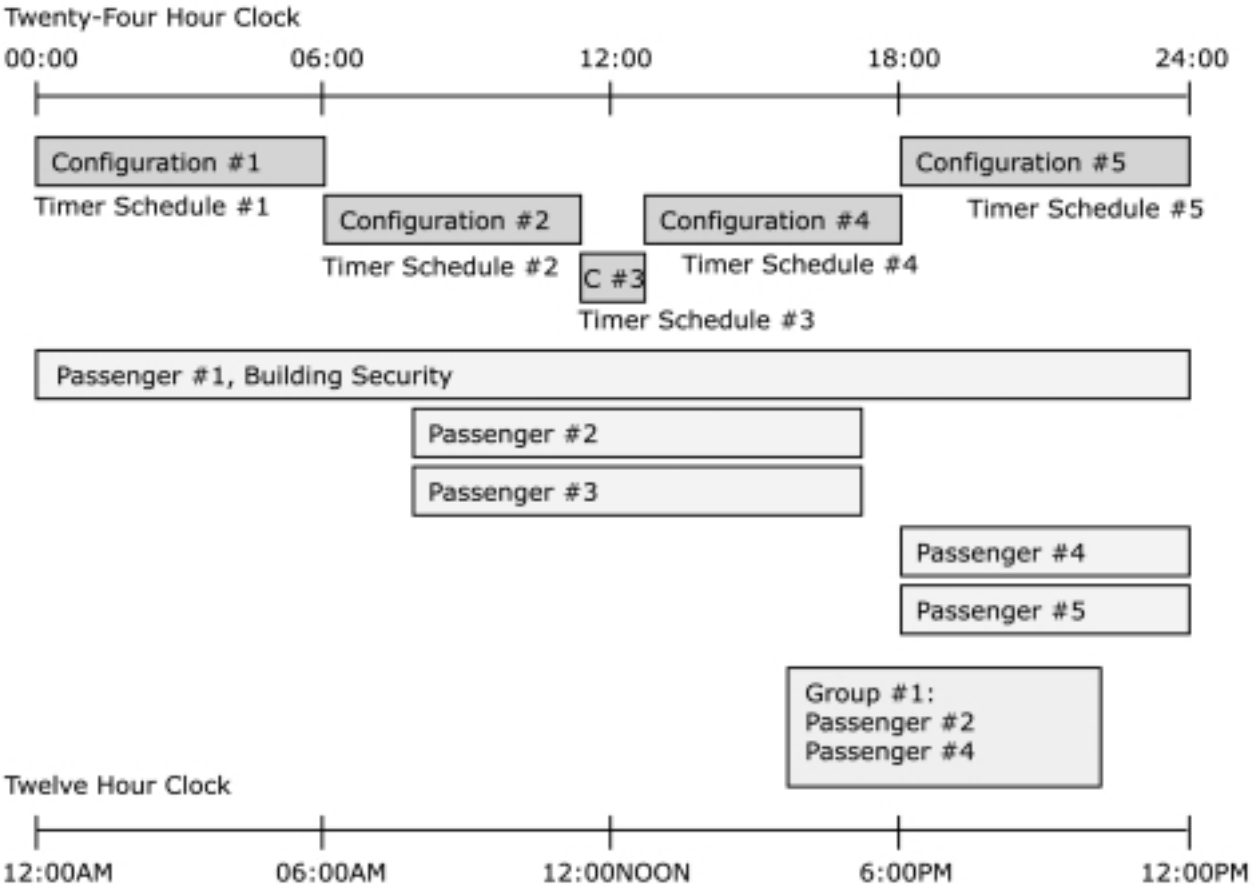
6. Set the car calls for the selected elevator for access to the associated floor.
   - U: Unsecured – Normal, unrestricted operation.
   - L: Locked – No access. The car call will not be registered for access to this floor.
   - S: Secured – Restricted access. The car will access the selected floor only if a valid security code is entered into the car control panel (and, for ACE systems, during a period of time for which the individual or group timer allows that code access.)

NOTE: For Basic and Basic with CRT security systems, a floor cannot be secured unless a security code has been programmed into the individual Car Controller's Main Computer. Refer to Viewing and Changing the Security Code in Section 2 (Basic) or Section 3 (Basic with CRT) respectively.

Floors for which a security code and a Security Configuration have been programmed are *secured* when that configuration is active and security is ON. In order to gain access to a secured floor via the elevator, the correct security code must be entered using the Car Operating Panel. When a car button for a secured floor is pressed, the button indicator will flash to indicate that a valid security code must be entered within ten seconds. If not, the call will not be registered.

7. Click **Save** to save changes to the Security Configuration or click **Close** before clicking Save to leave the dialog without accepting any unsaved changes.

The chart on the following page provides an example of the way Security Configurations, Timer Schedules, Passenger Personal Schedules, and Group Schedules interact to affect landing access when security is active.



Configurations:

- Define restricted and locked floors and elevator doors when active.
- Must be defined within a single 24 hour period - latest end time 23:59 (cannot cross Midnight)
- End times of 23:59 extend automatically to midnight

Passenger Schedules Allow:

- Access to selected restricted floors
- During scheduled times
- With valid code entry

Group Schedules Allow (for passengers in Group):

- Access to their selected restricted floors
- During scheduled times
- With valid code entry
- Extends/adds to Personal Schedule

In the example above:

- Configurations and Timers #s 1 and 5 both restrict access to all floors above floor #1.
- Configurations and Timers #s 2 and 6 allow office floor access.
- Configuration and Timer #3 allow office and dining floor access.
- Passenger #1 (Security) has all-hour access to all floors with valid code entry.
- Passengers # 2 and 3 have access to office floors during normal working hours with valid code entry.
- Passengers # 4 and 5 have access to all floors during maintenance hours with valid entry.
- Group #1 allows Passenger #2 to extend access when needed and Passenger #4 to come in early when necessary.

7.3.5 EDITING TIMER TABLES

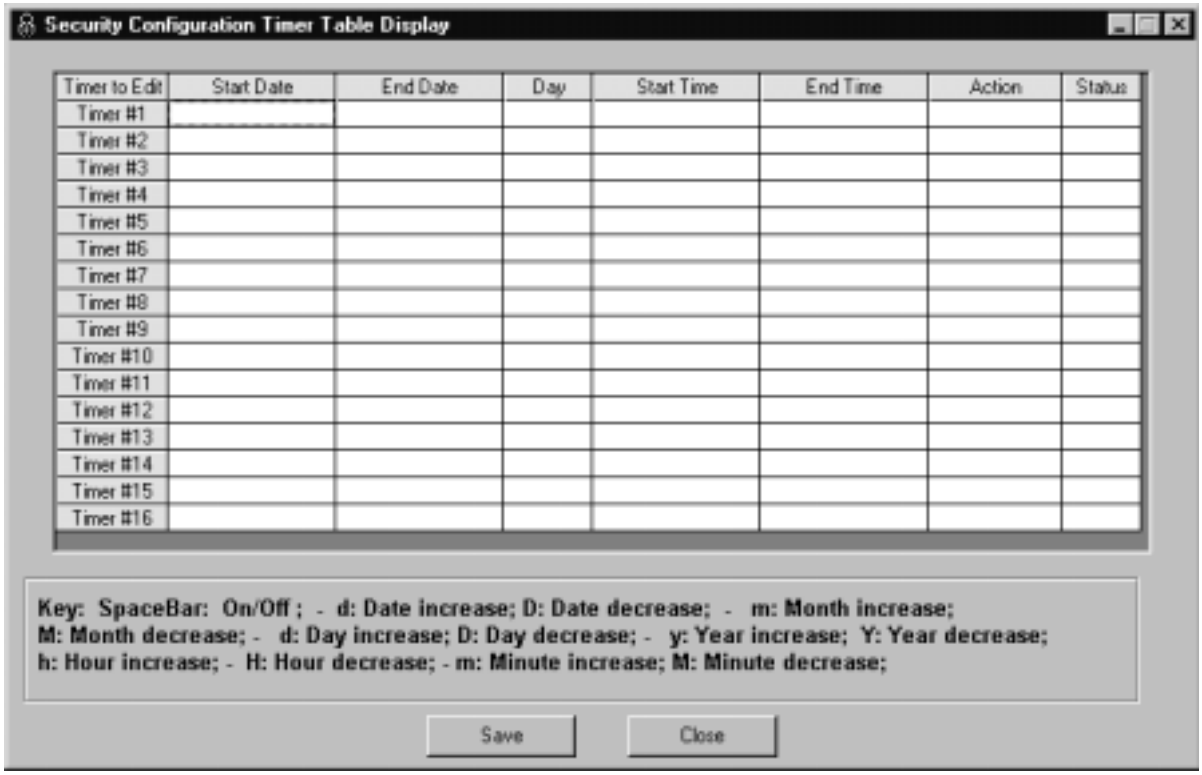
Through the Timer Table, you may set up as many as sixteen different schedules (Timers) for activating and deactivating Security Configurations. Once the Timer Table is configured, selecting timed operation (*Set Configuration Status*/*Timed* from the *Controller* menu, Section 7.3.6) causes it to begin automated control of the security system.

When timed/automated security is on, the controller continuously checks the status and settings of each of the sixteen timers. Timers that are active (On) have priority assignments that determine which Timer has priority if multiple Timers are on and their settings conflict. Timer #1 has highest priority; Timer #16 has lowest priority. For example, if Timers #1 and #6 were both on and were both set to control security all day on Mondays, Timer #1 would actually have control. Normally, Timer settings are complimentary and the controller switches from one Timer schedule to another as date/day/time settings warrant.

NOTE: If no Timers polled by the controller have a defined day and time period into which the current day and time fall, Security Configuration Status will be Timed OFF and Security Status will be OFF.

To set up Timers:

1. Select *Edit Timer Table* from the *Controller* menu to open the Timer Table.



Once you have set up a Timer, those settings (Start Time, End Time, etc.) will appear in the Timer Table. If supported by your controller, you will see and be able to set Date fields to enter specific start and end dates rather than by days of the week alone.

You edit the various fields by setting the Status field for that timer On, then clicking in the desired field and using specific edit keys. (You can also move from field to field using the keyboard up, down, left, and right arrow keys.) Save schedule changes by clicking on the Save button.

To set up a timer **using specific dates**:

1. Click in the Status field of the desired Timer.
2. Press the Space bar to switch that Timer Status to ON.
3. Click in the Action field.
4. Press the <c> key to increment through Security Configurations. (Use <Shift> <C> to decrement.)
5. Click in the Day field.
6. Press the <d> key to increment through the choices until DATE is displayed. (Use <Shift> <D> to decrement.)
7. Click in the Start Date field. Use the <m>, <d>, and <y> keys (Month/Day/Year) to increment months, days, and years respectively. (Use <Shift> and the <M>, <D>, or <Y> keys to decrement month, day, or year respectively.)
8. Click in the End Date field and use the <m>, <d>, and <y> keys as you did in the preceding step.
9. Click in the Start Time field. Use the <h> and <m> keys (Hours/Minutes) to increment hours and minutes respectively. (Use <Shift> <H> or <Shift> <M> to decrement hours and minutes respectively.)
10. Click in the End Time field. Use the <h> and <m> keys to set the time.
11. Click Save.

To set up a schedule **using days** rather than dates:

1. Click in the Status field of the desired Timer.
2. Press the Space bar to switch that Timer Status to ON.
3. Click in the Action field.
4. Press the <c> key to increment through Security Configurations. (Use <Shift> <C> to decrement.)
5. Click in the Day field.
6. Press the <d> key to increment through the choices until the desired day or day range is displayed. (Use <Shift> <D> to decrement.)
   - Mon, Tue, Wed, Thu, Fri, Sat, or Sun
   - M - F (Monday through Friday)
   - All (all days of the week)
7. Click in the Start Time field. Use the <h> and <m> keys (Hours/Minutes) to increment hours and minutes respectively. (Use <Shift> <H> or <Shift> <M> to decrement hours and minutes respectively.)
8. Click in the End Time field. Use the <h> and <m> keys to set the time.
9. Click Save.

Help - The dialog help button opens online help. The "Timer Entry" topic within repeats the entry key information provided below:

- Click in Status field then use the Space Bar to turn Timer ON or OFF.
- Click in the Action field, then use <c> to increment or <C> to decrement.
- Time: Click in Start or End Time field then use <h> or <m> to increment or <H> or <M> to decrement.
- Day: Click in Day field then use <d> to increment or <D> to decrement.
- Date: Click in Start or End Date field then use <m>, <d>, or <y> to increment months, days, and years respectively or <M>, <D>, or <Y> to decrement.
- Keyboard arrow keys may be used to move between fields.

CAUTION: Be careful not to define timers that overlap. If the *Start Time* of one timer is earlier than the *End Time* of another timer they may not operate as expected.

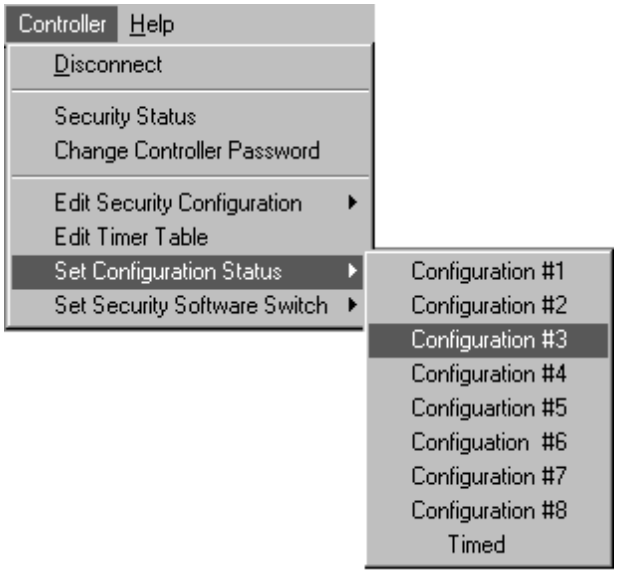
Example: Suppose you would like to use Security Configuration #5 overnight, from 20:00 (8 pm) to 6:00 (6 am) Monday through Friday. Use two timers and set the Day field of both timers to M-F. Set one timer's start time to 20:00 and end time to 23:59. Set the second timer's start time to 00:00, and End Time to 06:00. Set Config. # to 5 and Timer Status *ON* for both timers.

7.3.6 SETTING CONFIGURATION STATUS

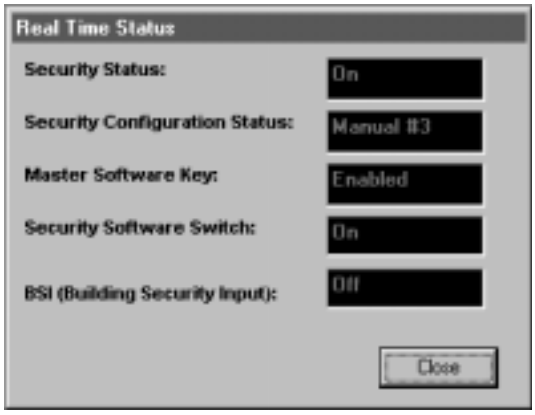
Once you have programmed one or more Security Configurations, you may select and activate Configurations manually or, if you have set up the Timer Table to control automated operation, you may select timed (automated) operation.

To select a Configuration manually:

1. Select *Set Configuration Status*/*Configuration #n* from the *Controller* menu.



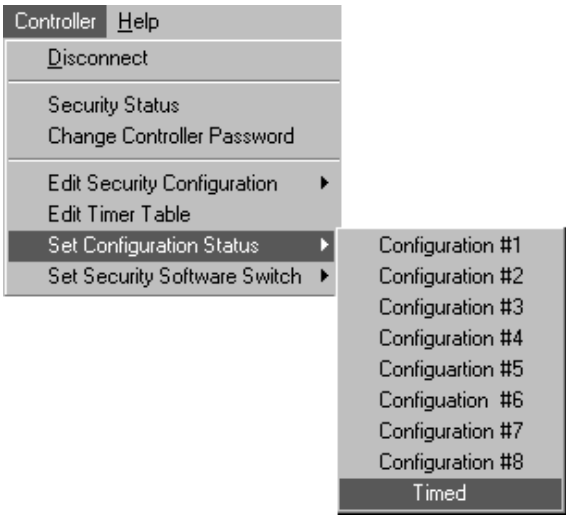
2. Check the Real Time Status display (*Controller*/*Security Status*) to see that the selected Configuration is active and indicates it was started manually.



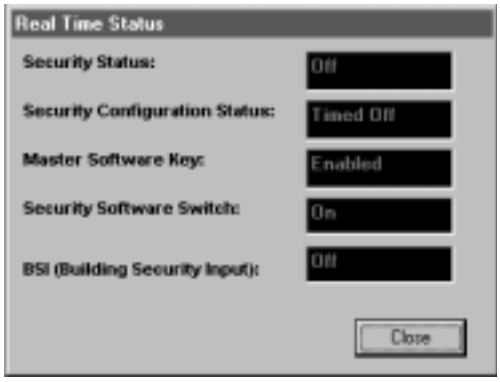
If Security Status in the Real Time Status display indicates that security is currently Off, you may switch it On by selecting *Set Security Software Switch*/*On* from the *Controller* menu.

To select automated operation:

1. Select *Set Configuration Status*/*Timed* from the *Controller* menu.



2. Check the Real Time Status display (*Controller*/*Security Status*) to see that status is as it should be according to the Security Configurations and Timer Table settings you have in place.

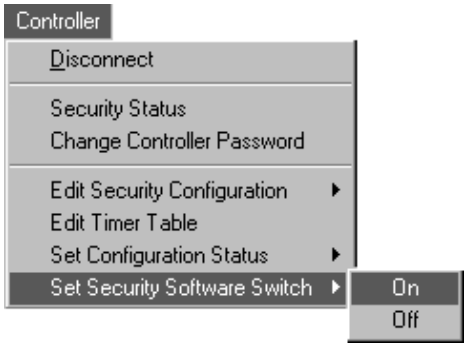


In the example above, if security was currently on, Security Status would indicate On and Security Configuration Status would indicate Timed #n (the number of the active Security Configuration).

7.3.7 SETTING THE SECURITY SOFTWARE SWITCH

When the Master Software Key is Enabled, the Security Software Switch and the optional Building Security Input enable security as shown in Table 7.1 earlier in this section. To set the Security Software Switch:

1. Select *Set Security Software Switch*/*On* or *Off* from the *Controller* menu.



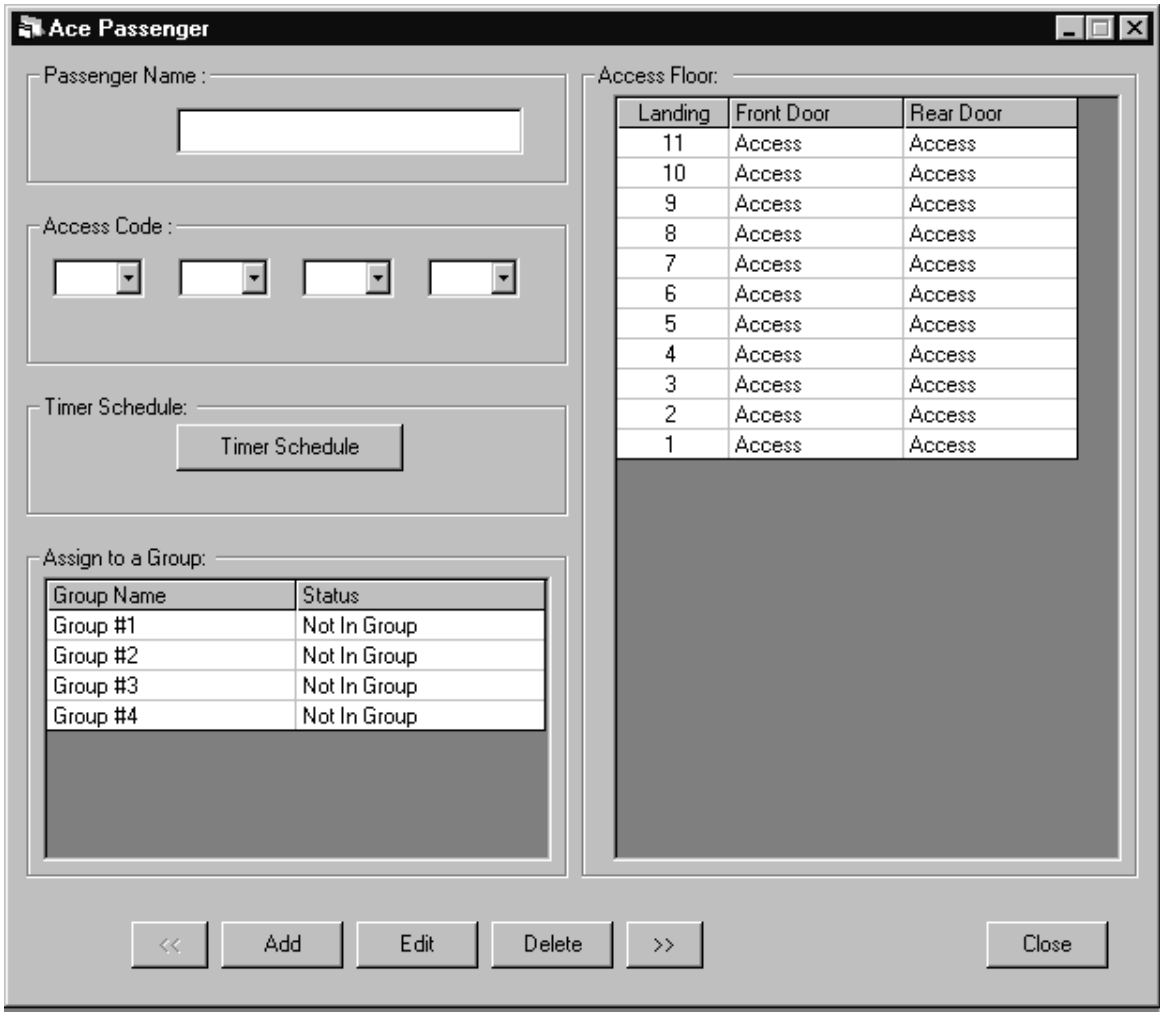
7.3.8 ENTERING PASSENGER DATA

This (ACE only) function allows you to set up individual profiles for elevator passengers, including:

- Modify Passenger Data
- Modify Group Data
- Set Length of Access Code (Set this before you assign access codes)

MODIFY PASSENGER DATA – This Controller menu selection allows you to add, edit, or delete passenger records.

- Select *Passenger Information Menu*/*Modify Passenger Data* from the *Controller* menu.



Add a Passenger – To add a new passenger:

1. Click on Add to enable Passenger Name field editing.
2. Enter the passenger name in the Passenger Name field.
3. Enter additional data (Access Code, Restrictions, etc.) as needed.
4. Click on Save.

Edit a Passenger – To edit existing passenger information:

1. Select the passenger using the left and right arrow buttons to cycle through names.
2. Click on Edit.
3. Edit the passenger name, access code, floor restrictions, timer schedule, or group assignments as described in this section.
4. Save your changes.

Assign or Change an Access Code – To assign or change a passenger Access Code:

1. Select the passenger using the left and right arrow buttons to cycle through names.
2. Click on Edit.
3. Click on the drop-down list arrow next to each Access Code entry field and set the code as desired.

Access Codes are from two to eight entries long. The **Access Code length should be set before any Passenger Access Codes are entered.** The characters you see in the drop-down lists are keyed to the floor selections in the installation so that they correspond to car operating panel buttons. For example, if there are six floors in the building, numbered from one to six, you would be able to select 1, 2, 3, 4, 5, or 6 for each entry position. If there are three floors in the building, labeled B, L, and 2, you would be able to select B, L, or 2 for each entry position. If there are floors in the building identified by more than one character and/or digit, for example 26 or L7, that character set would constitute one entry. Each entry is, of course, a single button press on the car operating panel.

4. Save your changes.

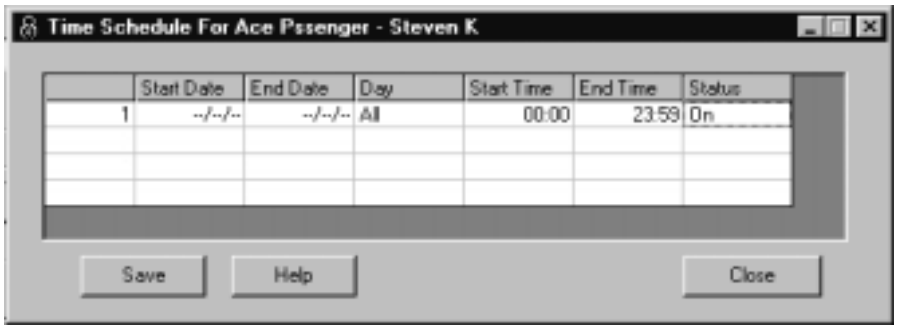
NOTE: To successfully access a restricted floor, a passenger must enter a valid access code, their floor restriction map must allow them access to that floor, and their individual or group timer schedule must grant access during the period of time in question.

Enter Floor Access Restrictions – To restrict passenger access to any floor:

1. Select the passenger using the left and right arrow buttons to cycle through names.
2. Click on Edit.
3. Click in the Front Door or Rear Door field for the desired landing.
4. Click the mouse to set the field to **Access** or **No Access** as desired.
5. Save your changes.

Edit Personal Timer Schedule – You may edit a selected passenger's personal timer schedule. The personal timer schedule determines the times the passenger may access the elevator. This allows the building manager the flexibility to provide a passenger access to the elevator during off-hours or weekends.

1. Select the passenger using the left or right arrow buttons to cycle through names.
2. Click the Timer Schedule button.
3. Click in the Status field of the desired schedule (up to four).



4. Press the Space bar to switch that schedule Status to ON.
5. Click in the Day field.
6. Press the <d> key to increment through the choices until the desired day or day range is displayed. (Use <Shift> <D> to decrement.)
   - Mon, Tue, Wed, Thu, Fri, Sat, or Sun
   - M - F (Monday through Friday)
   - All (all days of the week)
   - Date: Use Start and End Date fields instead of days.
7. Click in the Start Time field. Use the <h> and <m> keys (Hours/Minutes) to increment hours and minutes respectively. (Use <Shift> <H> or <Shift> <M> to decrement hours and minutes respectively.)
8. Click in the End Time field. Use the <h> and <m> keys to set the time.
9. Click in the Start Date field. Use the <m>, <d>, and <y> keys (Month/Day/Year) to increment months, days, and years respectively. (Use <Shift> and the <M>, <D>, or <Y> keys to decrement month, day, or year respectively.)
10. Click in the End Date field and use the <m>, <d>, and <y> keys as you did in the preceding step.
11. Click Save.

Help - The dialog help button opens online help. The “Timer Entry” topic within repeats the entry key information provided below:

- Click in Status field then use the Space Bar to turn schedule ON or OFF.
- Time: Click in Begin or End field then use <h> or <m> to increment or <H> or <M> to decrement.
- Day: Click in Day field then use <d> to increment or <D> to decrement.
- Date: Click in Start or End Date field then use <m>, <d>, or <y> to increment months, days, and years respectively or <M>, <D>, or <Y> to decrement.
- Keyboard arrow keys may be used to move between fields.

Assign a Passenger to a Group – A passenger, and his or her Passenger Access Code, may be assigned to any of four groups. Each group has an associated Time Schedule. A Group Time Schedule has sixteen timers so up to sixteen time periods may be defined. These time periods are additions to the time periods defined in the passenger’s personal time schedule. When determining access rights, the controller first checks the personal schedule and, if access is not permitted there, next checks the group schedule for all groups to which the passenger has been assigned.

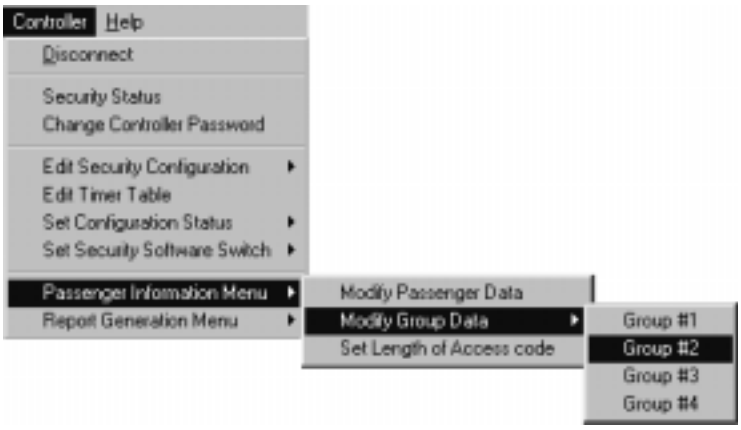
1. Select the passenger using the left or right arrow buttons to cycle through names.
2. Click on Edit.
3. In the *Assign to a Group:* pane, click in the *Status* field associated with the desired Group and set it to *Not In Group* or *In Group* as desired.
4. Save your changes.

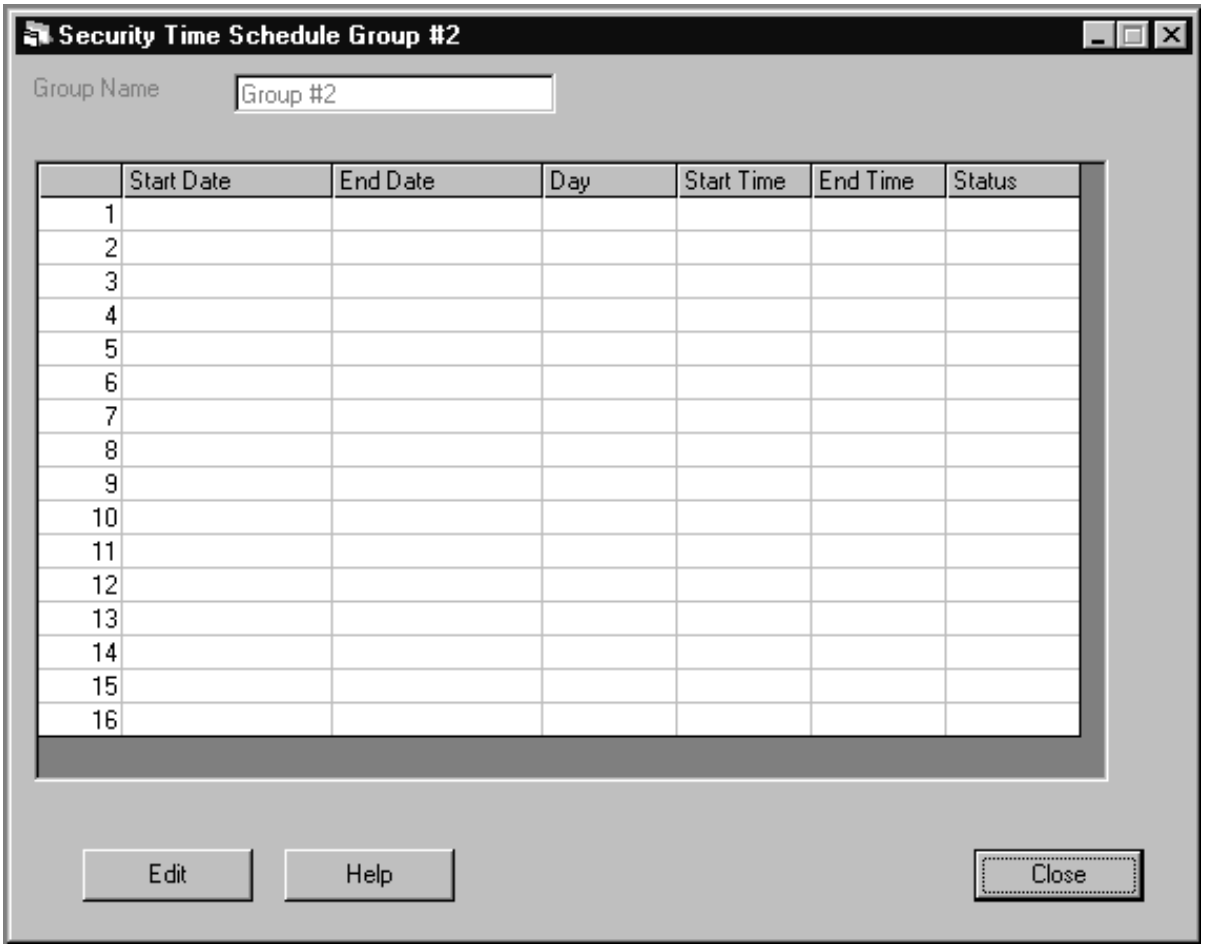
Delete a Passenger Record – You may permanently remove a passenger from the passenger list.

1. Select the passenger using the left or right arrow buttons to cycle through names.
2. Click on Edit.
3. Click *Delete*.
4. Verify that the passenger is to be deleted.
5. Save your changes.

MODIFY GROUP DATA – This Controller menu option allows you to edit Group properties.

- Select *Passenger Information Menu/Modify Group Data/Group #n* from the *Controller* menu.





Click on the dialog Help button to see a description of the keyboard keys used to edit the dialog settings.

Edit a Group Name – You may edit a Group name at any time.

1. Select the Group (*Passenger Information Menu/Modify Group Data/Group #n* from the *Controller* menu).

2. Click *Edit* to enable changes.

3. Edit the name in the *Group Name* field.

4. *Save* your changes.

Modify a Group Timer Schedule -- You may configure up to sixteen different schedules for each Group. If you choose to use date rather than day settings, the Start Date and End Date fields are active. If you choose to use day settings, the Start and End Date fields are inactive. You edit the various fields by setting the Status field for that schedule On, then clicking in the desired field and using specific edit keys. (You can also move from field to field using the keyboard up, down, left, and right arrow keys.) Save schedule changes by clicking on the Save button.

To set up a schedule **using specific dates**:

1. Click the Edit button.

2. Click in the Status field of the desired schedule.

3. Press the Space bar to switch that schedule Status to ON.

4. Click in the Day field.

5. Press the <d> key to increment through the choices until DATE is displayed. (Use <Shift> <D> to decrement.)

6. Click in the Start Date field. Use the <m>, <d>, and <y> keys (Month/Day/Year) to increment months, days, and years respectively. (Use <Shift> and the <M>, <D>, or <Y> keys to decrement month, day, or year respectively.)

7. Click in the End Date field and use the <m>, <d>, and <y> keys as you did in the preceding step.

8. Click in the Start Time field. Use the <h> and <m> keys (Hours/Minutes) to increment hours and minutes respectively. (Use <Shift> <H> or <Shift> <M> to decrement hours and minutes respectively.)

9. Click in the End Time field. Use the <h> and <m> keys to set the time.

10. Click Save.

To set up a schedule **using days** rather than dates:

1. Click the Edit button.
2. Click in the Status field of the desired schedule.
3. Press the Space bar to switch that schedule Status to ON.
4. Click in the Day field.
5. Press the <d> key to increment through the choices until the desired day or day range is displayed. (Use <Shift> <D> to decrement.)
   - Mon, Tue, Wed, Thu, Fri, Sat, or Sun
   - M - F (Monday through Friday)
   - All (all days of the week)
6. Click in the Start Time field. Use the <h> and <m> keys (Hours/Minutes) to increment hours and minutes respectively. (Use <Shift> <H> or <Shift> <M> to decrement hours and minutes respectively.)
7. Click in the End Time field. Use the <h> and <m> keys to set the time.
8. Click Save.

Help - The dialog help button opens online help. The “Timer Entry” topic within repeats the entry key information provided below:

- Click in Status field then use the Space Bar to turn schedule ON or OFF.
- Time: Click in Start or End Time field then use <h> or <m> to increment or <H> or <M> to decrement.
- Day: Click in Day field then use <d> to increment or <D> to decrement.
- Date: Click in Start or End Date field then use <m>, <d>, or <y> to increment months, days, and years respectively or <M>, <D>, or <Y> to decrement.
- Keyboard arrow keys may be used to move between fields.

SET LENGTH OF ACCESS CODE – Access code length may be set from two to eight entries. All access codes administered by the controller are proscribed to the same length. The Access Code length should be set before any Passenger Access Codes are entered. ACE Security should be OFF before Access Code Length changes are made. To set access code length:

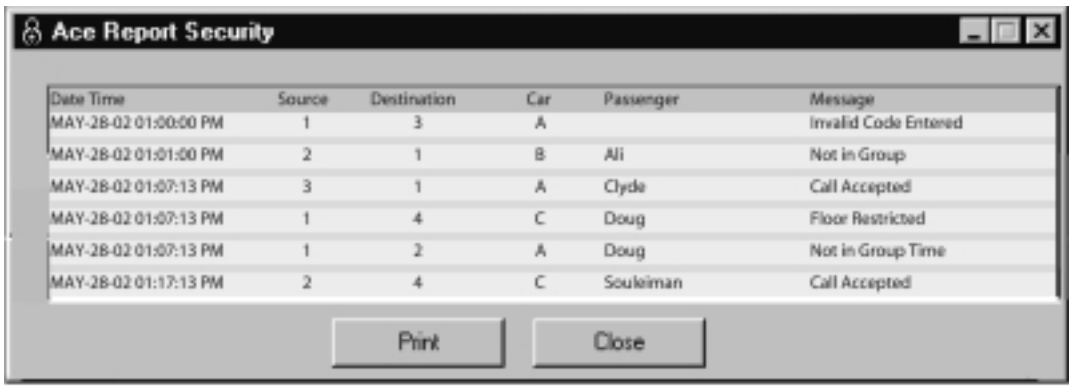
- From the *Controller* menu, select *Passenger Information Menu/Set Length of Access Code/Set Length 2 through 8*.

7.3.9 REPORT GENERATION MENU

The Report Generation Menu allows you to generate a list of the last (up to) 500 secured car calls registered. If a list is not cleared before it exceeds 500 entries then, as each new call is registered, the oldest call in the list will be deleted. Through the Report Generation Menu, you may:

- Generate a Security Report
- Clear the Security Report

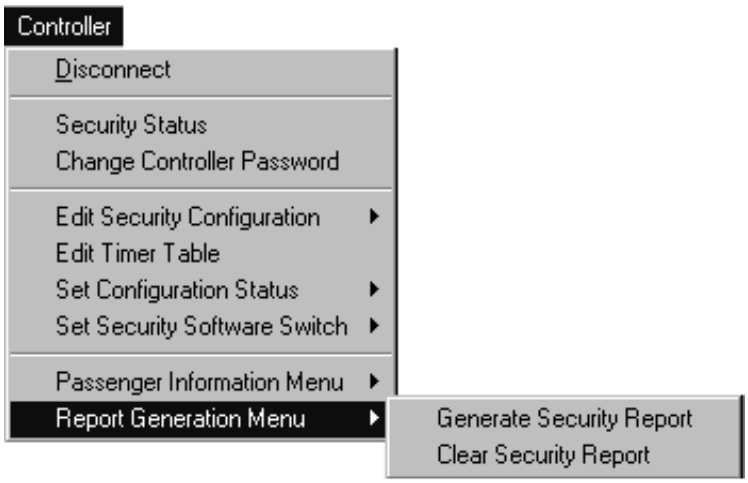
GENERATE A SECURED CAR CALL REPORT – A Secured Call Entry Report lists the date, time, source and destination floors, car, passenger, and accepted/rejected outcome for each call made for a secured car in the following format:



If desired, you may print the security report.

To generate a report:

1. Select *Report Generation Menu/Generate Security Report* from the *Controller* menu.



CLEAR SECURITY REPORT – This function allows you to clear the list of all car calls on the elevator controller.

1. Select *Report Generation Menu/Clear Security Report* from the *Controller* menu.
2. Verify that you wish to delete the list.
3. Click *Delete*.

7.3.10 DISCONNECTING FROM A CONTROLLER

When you are ready to disconnect from the elevator controller:

1. Select *Disconnect* from the *Controller* menu.

If you are ready to exit the program:

1. Select *Close* from the *File* menu.

7.4 THE HELP MENU

The Help menu provides quick access to on line help and to software version information.

Help – Select to open on line help.

Version – Select to check your software version.

APPENDIX
ELEVATOR SECURITY INFORMATION AND OPERATION

Building name: _____

Building location: _____

Security activation:	Key switch	Mon:	from _____	to ____
	or	Tue:	from _____	to ____
	Time clock	Wed:	from _____	to ____
		Thu:	from _____	to ____
		Fri:	from _____	to ____
		Sat:	from _____	to ____
		Sun:	from _____	to ____

Instructions: To gain access to secured floors, follow the steps below while in the elevator car. The steps may be taken while the car is moving or standing still. Requests for a car from a hallway or corridor are answered without restriction.

1. While in the car, press the button for the desired floor. If the destination floor is secured, the button for that floor will flash on/off.

   If the button for that floor stays solidly lit, that floor is unsecured.

2. While the destination floor button is flashing, enter the security code for that floor within 10 seconds. Enter the security code by pressing the corresponding buttons on the panel.

   If the code was entered correctly and within the required time limit, the car will immediately go to that floor. If the code was not entered within the 10-second time limit or was entered incorrectly, the destination floor button light will turn off after 10 seconds and the entire sequence must be repeated.

   If a mistake is made while entering the security code, simply wait until the destination floor button light stops flashing and start the entire sequence again.

SECURITY CODES

Maintain a record of the security codes by noting the floor name as found in the elevator cab and each floor's code. Any floor with a security code is a secured floor.

1.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
2.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
3.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
4.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
5.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
6.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
7.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
8.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
9.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
10.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
11.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
12.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
13.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
14.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
15.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
16.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
17.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
18.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
19.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
20.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
21.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
22.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
23.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
24.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
25.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
26.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
27.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
28.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
29.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
30.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
31.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
32.	**Floor**	_____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___

33.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
34.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
35.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
36.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
37.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
38.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
39.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
40.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
41.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
42.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
43.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
44.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
45.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
46.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
47.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
48.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
49.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
50.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
51.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
52.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
53.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
54.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
55.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
56.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
57.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
58.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
59.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
60.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
61.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
62.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
63.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___
64.	**Floor** _____	**security code**	**=**	___ ___ ___ ___ ___ ___ ___ ___

This page intentionally blank

INDEX

Access Control for Elevators (ACE) Security, 5-1, 5-27
assigning Passenger Access Codes (PAC), 5-16
BSI, Building Security Input, 5-8
changing a Group Name, 5-24
description, 1-2, 5-1, 5-3-6
Floor Map, 5-16, 5-21
Group Assignment Table, 5-17
List Secured Car Calls Registered, 5-26
lost or forgotten password, 5-11
on Security Interface Software (SIS), 6-11, 6-18, 7-31
Personal Time Schedule, 5-16, 5-20
programming a Group Time Schedule, 5-22
programming checklist, 5-27
programming the password, 5-10
programming the Security Configuration Timer Table, 5-14
programming the Security Configurations, 5-11, 5-12
Security Configuration Status, 5-9
Security Reports, 5-25
Security Software Switch, 5-8
setting the Master Software Key, 5-6
setting the PAC size, 5-18
turning security ON or OFF, 5-6

Basic Security
programming the Security Codes (PTC, PHC), 2-3
programming the Security Codes (Swing Panel), 2-4
turning ON and OFF, 2-1

Basic Security with CRT
description of, 1-2, 3-1, 4-1
on PTC and PHC controllers, 4-1-7, 4-9-11, 4-13, 4-14, 4-15, 4-16
on Security Interface Software (SIS), 6-10, 7-31
on Swing Panel controllers, 3-1-4, 3-6-13, 3-16-18
programming checklist (PTC, PHC), 4-16
programming checklist (Swing Panel), 3-17
programming the password (PTC, PHC), 4-10
programming the password (Swing Panel), 3-9
programming the Security Codes (PTC, PHC), 4-15, 4-16
programming the Security Codes (Swing Panel), 3-16
programming the Security Configuration Timer Table (PTC, PHC), 4-12-14
programming the Security Configuration Timer Table (Swing Panel), 3-13
programming the Security Configurations (PTC, PHC), 4-11
programming the Security Configurations (Swing Panel), 3-10
turning ON and OFF (PTC, PHC)), 4-5
turning ON and OFF (Swing Panel), 3-6

Building Security Input (BSI)
on Access Control for Elevators (ACE), 5-8
on Basic Security with CRT (PTC, PHC), 4-7
on Basic Security with CRT (Swing Panel), 3-8
on Security Interface Software (SIS), 6-12
on Security Interface Software for Windows, 7-8

Group Time Schedule
Access Control for Elevators (ACE) Security, 5-22
on Security Interface Software (SIS), 6-23
on Security Interface Software for Windows, 7-27

Master Software Key (MSK)
on Access Control for Elevators (ACE), 5-6
on Basic Security with CRT (PTC, PHC), 4-5, 4-6
on Basic Security with CRT (Swing Panel), 3-6, 3-7
on PTC and PHC controllers, 2-1
on Security Interface Software (SIS), 6-12

Master Software Key (MSK)
on Security Interface Software for Windows, 7-8

MCE's Elevator Security
overview, 1-4

Passenger Access Code (PAC)
Access Control for Elevators (ACE) Security, 5-16
assigning Passenger Access Codes (PAC), 5-20
on Security Interface Software for Windows, 7-23
setting the PAC size, 5-18

Passenger Information Database
Access Control for Elevators (ACE) Security, 5-18
on Security Interface Software (SIS), 6-18-22
on Security Interface Software for Windows, 7-22

Password
on Access Control for Elevators (ACE), 5-3, 5-10
on Basic Security with CRT (PTC, PHC), 4-2, 4-10
on Basic Security with CRT (Swing Panel), 3-2, 3-9
on Security Interface Software (SIS), 6-27
on Security Interface Software for Windows, 7-10

Per-Car Hall Call Security, 3-11-12, 6-14

Programming checklist
on Access Control for Elevators (ACE), 5-27
on Basic Security with CRT (PTC, PHC), 4-16
on Basic Security with CRT (Swing Panel), 3-17

Security codes
on Basic Security with CRT (PTC, PHC), 4-15, 4-16
on Basic Security with CRT (Swing Panel), 3-16, 3-17
on PTC and PHC controllers, 2-3
on Swing Panel controllers, 2-4

Security Configuration Status
on Access Control for Elevators (ACE), 5-9
on Basic Security with CRT (PTC, PHC), 4-3, 4-7
on Basic Security with CRT (Swing Panel), 3-4, 3-8
on Security Interface Software (SIS), 6-12
on Security Interface Software for Windows, 7-8

Security Configuration Timer Table, 4-13
on Access Control for Elevators (ACE), 5-14
on Basic Security with CRT (PTC, PHC), 4-3, 4-12-14
on Basic Security with CRT (Swing Panel), 3-4, 3-13, 3-14
on Security Interface Software (SIS), 6-15
on Security Interface Software for Windows, 7-16

Security Configurations
on Access Control for Elevators (ACE), 5-11
on Basic Security with CRT (PTC, PHC), 4-3, 4-11
on Basic Security with CRT (Swing Panel), 3-4, 3-10, 3-11
on Security Interface Software (SIS), 6-12-14
on Security Interface Software for Windows, 7-11

Security Interface Software (SIS), 6-1, 6-27, 7-31
com port setup, 6-4, 6-5, 6-8
description of, 1-3, 6-1
job connection settings, 6-3, 6-5, 6-8, 7-3
programming the Security Configuration Timer Table, 6-15, 6-16
programming the Security Configurations, 6-12-14

Security Interface Software (SIS) , 6-18, 6-27
programming the Group Data, 6-23
programming the Group Time Schedule, 6-24
programming the Passenger Access Codes (PAC), 6-20
programming the passenger information, 6-18-20
programming the password, 6-27
programming the Personal Time Schedule, 6-21
Security Reports, 6-25
setting the PAC size, 6-25

Security Interface Software (SIS) for Windows, 7-1
Add a new passenge, 7-23
Add or Delete Job Setups, 7-5
Assign a Passenger to a Group, 7-25
Assign Access Code, 7-23
Building Security Input, 7-8
Change Controller Password, 7-10
Communication Media, 7-4
Connect to a controller, 7-7
Connection Choices, 7-3
Controller menu, 7-6
Delete a Passenger Record, 7-25
DIGI Port and CoBox device servers, 7-5
Disconnect from Controller, 7-30
Edit a Group Name, 7-27
Edit existing passenger, 7-23
Edit Group properties, 7-26
Edit Personal Timers, 7-24
Editing Timer Tables, 7-16
Entering Timer data, 7-18
Generate Secured Car Call Report, 7-29
Initialize Controller List, 7-30
Installation, 7-2
Job Configuration, 7-3
Lost Password, 7-7, 7-8
Master Software Key, 7-8
Modem Configuration, 7-5
Modify a Group Timer Schedule, 7-27
Modify Passenger Data, 7-22
Per car Security Configuration, 7-13
Personal timer entry keys, 7-25
Real Time Status display, 7-8
Report Generation, 7-29
Restrict passenger access, 7-24
Security Configurations, 7-11
Security Software Switch, 7-8
Security Status Decision Matrix, 7-9
Security Timing Chart, 7-15
Select automated operation, 7-20
Set Access Code length, 7-28
Set Configuration Status, 7-19
Set Security Software Switch, 7-21
Stand alone installation, 7-2
System Requirements, 7-2
Timer entry keys, 7-18
Timer Priority, 7-16

Security Reports
List Secured Car Calls Registered, 5-26
on Security Interface Software for Windows, 7-29

Security Software Switch
on Access Control for Elevators (ACE), 5-5, 5-8
on Basic Security with CRT (PTC, PHC), 4-4, 4-7
on Basic Security with CRT (Swing Panel), 3-5, 3-7
on Security Interface Software (SIS), 6-12, 6-18
on Security Interface Software for Windows, 7-21

Security Status
on Access Control for Elevators (ACE), 5-5
on Basic Security with CRT (PTC, PHC), 4-4
on Basic Security with CRT (Swing Panel), 3-5
on Security Interface Software (SIS), 6-12
on Security Interface Software for Windows, 7-8

Turning security ON and OFF
on Access Control for Elevators (ACE), 5-6, 5-7
on Basic Security with CRT (PTC, PHC), 4-5, 4-6
on Basic Security with CRT (Swing Panel), 3-6