

# SE 6000

*SECURITY  
MANAGEMENT  
SYSTEM*

## STANDARD PRODUCT MANUAL



**Westinghouse  
Security Electronics**

*an ISO 9001 certified company*

5452 Betsy Ross Drive  
Santa Clara, CA 95054-1184  
(408) 727-5170  
FAX (408) 727-6707

P/N 66107919001, Rev. F

## LIMITED WARRANTY

Westinghouse Security Electronics (WSE) warrants to the original user the equipment manufactured by WSE as described herein (the equipment) to be free from defects in material and workmanship for a period of one year from the date of purchase by such user or fifteen (15) months from the date of shipment from the factory, whichever is sooner, provided:

- I WSE has been notified within such period by return of any alleged defective equipment, free and clear of any liens and encumbrances to WSE or its authorized Dealer at the address specified, transportation prepaid; and
- II the equipment has not been abused, misused or improperly maintained and/or repaired during such period; and
- III such defect has not been caused by ordinary wear and tear; and
- IV such defect is not a result of voltage surges/brownouts, lightning, water damage/flooding, fire, explosion, earthquakes, tornadoes, acts of aggression/war or similar phenomena; and
- V accessories used as an integral to WSE systems have been approved by WSE (e.g., coaxial cables, batteries, etc.); and
- VI the equipment has been installed, the installation supervised or installation tested by an authorized WSE dealer.

WSE's Proximity Command Keys are warranted for 5 years. WSE shall at its option, either repair or replace, free of charge, the equipment found, upon WSE's inspection to be so defective, or if agreed upon, refund the purchase price, less a reasonable allowance for depreciation, in exchange for the equipment. Magnetic Stripe Cards are warranted as described by the manufacturer's warranty.

WSE makes no other warranty, and all implied warranties including any warranty of merchantability or fitness for a particular purpose are limited to the duration of the expressed warranty period as set forth above.

WSE's maximum liability hereunder is limited to the purchase price of the equipment. In no event shall WSE be liable for any consequential, indirect, incidental or special damages of any nature arising from the sale or use of the product.

Some states do not allow limitations on incidental or consequential damages or how long an implied warranty lasts, so the above limitations may not apply. This warranty gives specific legal rights; however, other rights which vary from state to state, may pertain.

## IMPORTANT

The information provided in this manual is believed to be accurate and reliable. However, Westinghouse Security Electronics (WSE) assumes no responsibility for any errors that may appear. Possession of this manual does not imply the granting of licenses to make or sell equipment or software constructed according to descriptions provided.

# TABLE OF CONTENTS

|   |            |
|---|------------|
| <b>SECTION 1: INTRODUCTION .....</b>              | <b>1-1</b> |
| MANUAL ORGANIZATION .....                         | 1-1        |
| System Main Menu .....                            | 1-1        |
| Documentation Methods .....                       | 1-2        |
| DEFINITIONS .....                                 | 1-2        |
| General .....                                     | 1-2        |
| System Hardware — Devices .....                   | 1-3        |
| System Software .....                             | 1-5        |
| Principal System Functions .....                  | 1-6        |
| SAMPLE SYSTEM .....                               | 1-7        |
| CREATING THE DATABASE .....                       | 1-8        |
| BASIC SYSTEM USAGE .....                          | 1-9        |
| Logging On .....                                  | 1-9        |
| System Screens .....                              | 1-10       |
| Application Screens .....                         | 1-10       |
| SCREEN EXAMPLES .....                             | 1-11       |
| USING SCREENS AND FIELDS .....                    | 1-12       |
| Selecting Screens .....                           | 1-12       |
| Moving Between Data Fields .....                  | 1-12       |
| Moving to Prior Screens .....                     | 1-13       |
| FINDING, ADDING, AND STORING DATA .....           | 1-13       |
| Finding Data .....                                | 1-13       |
| Searching With Partial Information .....          | 1-13       |
| Adding / Changing Data .....                      | 1-14       |
| Storing Data .....                                | 1-14       |
| DELETING RECORDS .....                            | 1-14       |
| ZOOM FEATURE .....                                | 1-15       |
| Cancel Zoom .....                                 | 1-15       |
| MISCELLANEOUS INFORMATION .....                   | 1-15       |
| LOGGING OFF .....                                 | 1-15       |
| SHUTTING DOWN .....                               | 1-16       |
| RESTARTING .....                                  | 1-16       |
| Automatic Restart .....                           | 1-16       |
| Manual Restart .....                              | 1-16       |
| SYSTEM SCREEN TREES .....                         | 1-17       |
| Appendix A: System Screen Trees .....             | 1-17       |
| Appendix B: System Screen Hierarchies .....       | 1-17       |
| OPTIONAL FEATURES .....                           | 1-17       |
| <br>  |            |
| <b>SECTION 2: MONITOR SECURITY ACTIVITY .....</b> | <b>2-1</b> |
| INTRODUCTION .....                                | 2-1        |
| SECTION ORGANIZATION .....                        | 2-1        |
| FUNCTION KEYS .....                               | 2-2        |
| DATA ITEM SELECTION .....                         | 2-2        |
| CONTROL FUNCTIONS MENU .....                      | 2-2        |
| Pollers .....                                     | 2-2        |
| Devices .....                                     | 2-3        |
| Locks .....                                       | 2-4        |
| Input Points .....                                | 2-5        |
| Output Points .....                               | 2-5        |

|   |            |
|---|------------|
| Doors .....                                       | 2-6        |
| Select Zone .....                                 | 2-6        |
| REVIEW TRANSACTIONS (FULL SCREEN) .....           | 2-7        |
| ALARM SERVICING .....                             | 2-8        |
| REAL TIME CONTROL MAPS .....                      | 2-8        |
| CONTROL PROJECTS .....                            | 2-9        |
| ABORT TIMERS .....                                | 2-9        |
| OTHER FUNCTIONS .....                             | 2-9        |
| Printer Control .....                             | 2-9        |
| Forgive Passback .....                            | 2-10       |
| Manual Access Granted .....                       | 2-10       |
| Force Table Download .....                        | 2-10       |
| Remote Devices .....                              | 2-11       |
| Building Modes .....                              | 2-11       |
| Full Screen Monitoring .....                      | 2-12       |
| MISCELLANEOUS INFORMATION .....                   | 2-12       |
| Disk Almost Full Warning .....                    | 2-12       |
| Status Screen Function Timeout .....              | 2-13       |
| Alarm Servicing — No Activity Timeout .....       | 2-13       |
| Monitoring Security - Passwords .....             | 2-14       |
| Modified Usage of Invalid Facility Code Log ..... | 2-15       |
| <b>SECTION 3 SECURITY REPORTS .....</b>           | <b>3-1</b> |
| INTRODUCTION .....                                | 3-1        |
| POINT HISTORY REPORT .....                        | 3-2        |
| Point History — Sample Report .....               | 3-2        |
| KEYHOLDER HISTORY REPORT .....                    | 3-2        |
| Keyholder History — Sample Report .....           | 3-3        |
| TRANSACTION HISTORY REPORT .....                  | 3-3        |
| Transaction History — Sample Report .....         | 3-4        |
| ACCESS CONTROL ARCHIVE REPORT .....               | 3-4        |
| ALARM SERVICING REPORT .....                      | 3-4        |
| Alarm Servicing — Sample Report .....             | 3-5        |
| PASSBACK ZONE REPORT .....                        | 3-5        |
| Passback Zone — Sample Report .....               | 3-6        |
| DOWNLOAD STATUS REPORT .....                      | 3-6        |
| Download Status — Sample Report .....             | 3-7        |
| KEYHOLDER ZONE REPORT .....                       | 3-8        |
| Keyholder Zone — Sample Report .....              | 3-8        |
| EVENT / POINT REPORT .....                        | 3-8        |
| Event / Point — Sample Report .....               | 3-9        |
| REALTIME PASSBACK ZONE REPORT .....               | 3-9        |
| REALTIME PASSBACK DETAIL — SAMPLE REPORT .....    | 3-10       |
| <b>SECTION 4 MASTER FILE ENTRY .....</b>          | <b>4-1</b> |
| INTRODUCTION .....                                | 4-1        |
| Screen Access .....                               | 4-1        |
| KEYHOLDERS .....                                  | 4-2        |
| Keyholder Entry—Page 1 [key_entr] .....           | 4-2        |
| Keyholder Entry—Page 2 [key1entr] .....           | 4-4        |

|   |            |
|---|------------|
| Keyholder Access Entry [empgentr] .....                     | 4-5        |
| Project Assignment [epj_entr] .....                         | 4-6        |
| COPY KEYHOLDERS .....                                       | 4-7        |
| Copy Keyholder Information .....                            | 4-7        |
| ACCESS ASSIGNMENT .....                                     | 4-8        |
| Keyholder Access Assignment [egrpentr] .....                | 4-8        |
| COPY KEYHOLDER ACCESS [ERGCOPY] .....                       | 4-8        |
| ACCESS DEFINITION .....                                     | 4-9        |
| Access Code Entry [acdsentr] .....                          | 4-9        |
| Access Group Entry [agdsentr], [agrpentr] .....             | 4-11       |
| Access Override Entry .....                                 | 4-13       |
| Failsoft Entry .....  | 4-14       |
| Project Entry [prj_entr], [prd_entr] .....                  | 4-14       |
| TIME CODES [TMCDETR] .....                                  | 4-16       |
| HOLIDAYS [HOL_ENTR] .....                                   | 4-16       |
| TENANTS [TENTENTR] .....                                    | 4-17       |
| INSTRUCTIONS [INSTENTR] .....                               | 4-17       |
| HARDWARE CONFIGURATION [CONFMENU] .....                     | 4-18       |
| Zones [zoneentr] .....                                      | 4-18       |
| Areas [areaentr], [areaentr1] .....                         | 4-19       |
| Pollers [pol_entr] .....                                    | 4-19       |
| Devices .....   | 4-21       |
| Device Entry [dev_entr] — All Device Types .....            | 4-22       |
| SE NexSentry Device Configuration Entry [nexsentr] .....    | 4-26       |
| Readers .....   | 4-31       |
| Reader Entry [rdr_entr] .....                               | 4-32       |
| Points [pnt_entr] .....                                     | 4-39       |
| Auto Opens / Activates .....                                | 4-42       |
| Device Report Definition [rdefentr] .....                   | 4-43       |
| SE 422 PIN Definition .....                                 | 4-43       |
| SE 422 Hardware Definition .....                            | 4-44       |
| Dialer Entry .....  | 4-45       |
| Site Entry Definition .....                                 | 4-46       |
| ABA Configuration Entry .....                               | 4-47       |
| DKR Configuration Entry .....                               | 4-48       |
| USER-DEFINED INFORMATION .....                              | 4-49       |
| MAPS .....  | 4-50       |
| Map Drawing Commands and Descriptions .....                 | 4-50       |
| <b>SECTION 5: MASTER FILE REPORTS .....</b>                 | <b>5-1</b> |
| INTRODUCTION .....  | 5-1        |
| ADDITIONAL INFORMATION .....                                | 5-2        |
| KEYS MASTER .....   | 5-2        |
| Keyholder Quick List — Sample Report .....                  | 5-3        |
| Keyholder Holder Master Report — Sample Report .....        | 5-3        |
| ACCESS ASSIGNMENTS .....                                    | 5-4        |
| Keyholder Access Assignment .....                           | 5-4        |
| Keyholder Access Assignment: Regular — Sample Report .....  | 5-4        |
| Keyholder Access Assignment: Extended — Sample Report ..... | 5-5        |

|  |      |
|--|------|
| Reader Access Assignment .....                                 | 5-5  |
| Reader Assignment — Sample Report .....                        | 5-5  |
| ACCESS DEFINITION .....  | 5-6  |
| Access Code Master .....                                       | 5-6  |
| Access Group Master .....                                      | 5-6  |
| Access Override .....  | 5-7  |
| Intelligent Fail Soft Report .....                             | 5-7  |
| Project Report .....   | 5-8  |
| Keyholder Project Report .....                                 | 5-9  |
| Reader Project Report .....                                    | 5-10 |
| TIME CODES .....   | 5-10 |
| HOLIDAYS .....   | 5-11 |
| TENANTS .....  | 5-11 |
| Tenants — Sample Report .....                                  | 5-12 |
| COMPANY, DEPT, LOCATION, JOB CAT .....                         | 5-12 |
| Company, Dept, Location, Job Cat — Sample Company Report ..... | 5-12 |
| INSTRUCTIONS .....   | 5-12 |
| Sample Instructions .....                                      | 5-13 |
| MAPS .....   | 5-13 |
| Sample Report — Map Information .....                          | 5-13 |
| DEVICE CONFIGURATION REPORTS .....                             | 5-13 |
| Zones .....  | 5-13 |
| Zones — Sample Report .....                                    | 5-14 |
| Pollers .....  | 5-14 |
| Pollers — Sample Report .....                                  | 5-14 |
| Devices .....  | 5-14 |
| Devices — Sample Report .....                                  | 5-15 |
| Readers .....  | 5-15 |
| Readers — Sample Report .....                                  | 5-16 |
| Points .....   | 5-16 |
| Points — Sample Report .....                                   | 5-16 |
| Auto Opens / Activates .....                                   | 5-17 |
| Auto Open / Activate — Sample Report .....                     | 5-17 |
| 808 Report Definition .....                                    | 5-17 |
| 808 Report Definition — Sample Report .....                    | 5-17 |
| 808 Device Configuration .....                                 | 5-18 |
| 808 Device Configuration — Sample Report .....                 | 5-18 |
| Dialers .....  | 5-18 |
| Dialers — Sample Report .....                                  | 5-18 |
| Site Definition .....  | 5-18 |
| Site Definition — Sample Report .....                          | 5-19 |
| ABA Configuration .....  | 5-19 |
| ABA Configuration — Sample Report .....                        | 5-19 |
| DKR Configuration .....  | 5-20 |
| DKR Configuration — Sample Report .....                        | 5-20 |
| SE 422 PIN Master Report .....                                 | 5-20 |
| SE 422 PIN Master Report — Sample .....                        | 5-21 |
| 132-COLUMN REPORT DISPLAY .....                                | 5-21 |

|  |            |
|--|------------|
| <b>SECTION 6: SYSTEM ADMINISTRATION .....</b>        | <b>6-1</b> |
| INTRODUCTION .....                                   | 6-1        |
| SECTION ORGANIZATION .....                           | 6-1        |
| ADDITIONAL INFORMATION .....                         | 6-2        |
| ADD USERS [ADDUSERS] .....                           | 6-2        |
| MODIFY PASSWORDS [MOD_PASS] .....                    | 6-4        |
| PROGRAM SECURITY [SEC_MENU] .....                    | 6-5        |
| Program Security Level Entry [pgacentr] .....        | 6-5        |
| Program Security Entry Definition [pg1_entr] .....   | 6-5        |
| Copy Security [mnaccopy] .....                       | 6-6        |
| Security Master List [pgacrpt] .....                 | 6-6        |
| DISPLAY ALL VALID LOGINS [SHOWUSER] .....            | 6-7        |
| DISPLAY CURRENT DATE AND TIME [SHOWDATE] .....       | 6-7        |
| DISPLAY ALL USERS WHO ARE LOGGED IN [SHOWWHO] .....  | 6-7        |
| PURGE A PENDING REPORT [PURGRPT] .....               | 6-8        |
| ENABLE TERMINALS FOR GLOBAL BEEPING [BEEPENTR] ..... | 6-8        |
| SYSTEM CONFIGURATION (SYCLMENU) .....                | 6-8        |
| Control File Maintenance [ctrlentr] .....            | 6-8        |
| Events [evenentr] .....                              | 6-9        |
| Tasks [taskentr] .....                               | 6-10       |
| Task Event / Master Report [taskrpt] .....           | 6-12       |
| Transactions [tranentr] .....                        | 6-12       |
| DATABASE MAINTENANCE [DB_MENU] .....                 | 6-14       |
| Display Database Statistics [dbstats] .....          | 6-14       |
| Perform Backup [bkup] .....                          | 6-14       |
| Alarm Transaction Clean Up [alrmcln] .....           | 6-16       |
| Journal Archive [jourarch] .....                     | 6-16       |
| Journal Reporting [jourrpt] .....                    | 6-16       |
| Special Journal Reporting [josrprt] .....            | 6-16       |
| KEYHOLDER LOADING [LOADMENU] .....                   | 6-17       |
| ID SECURITY MAINTENANCE [ID_MENU] .....              | 6-17       |
| ID Security User Entry [ID1_entr] .....              | 6-17       |
| ID Security Group Entry [ID2_entr] .....             | 6-18       |
| ID Security Report [ID1_rprt] .....                  | 6-18       |
| MISCELLANEOUS INFORMATION .....                      | 6-19       |
| Adjustable Baud Rate—708P / 800 Pollers .....        | 6-19       |
| 708P REX Shunt Time Reset .....                      | 6-19       |
| Key Inventory [invtmnu] .....                        | 6-20       |
| Inventory Status Code Menu [statentr] .....          | 6-20       |
| Key Inventory Status Code Report [statrpt] .....     | 6-20       |
| Key Inventory Entry [cdinentr] .....                 | 6-21       |
| Key Inventory Report [cdinrpt] .....                 | 6-21       |
| PARKING STICKERS [STKRMENU] .....                    | 6-22       |
| Parking Sticker Entry [stkrentr] .....               | 6-22       |
| Parking Sticker Interactive Display [stkrprt1] ..... | 6-22       |
| Parking Sticker Master Report [stkrprt] .....        | 6-23       |

# SECTION 1

# INTRODUCTION

## MANUAL ORGANIZATION

This manual follows the order of the seven standard product items in the system main menu, with the *Key Inventory* and *Parking Stickers* items merged into the *System Administration* section:

- *Section 2: Monitor Security Activity*
- *Section 3: Security Management Reports*
- *Section 4: Master File Entry*
- *Section 5: Master File Reports*
- *Section 6: System Administration*

## System Main Menu



The system main menu is the departure point for accessing all other system screens (main menu screens may vary according to options purchased).

## Documentation Methods

To avoid repetition and to reduce document size, detailed explanations for the system's principal data items are given only in *Section 4: Master File Entry*, which is used when creating the system database. For introductory information concerning the data items, see *Definitions* below.

Further, with the exception of the screens presented in *Basic System Usage* in this section, and the introductory menu screens for *Sections 2* through *Section 5*, all other screens throughout this manual are limited to the particular screen area being discussed (i.e., full screens are not shown). In some cases, screen presentations are unnecessary and are not used.

## DEFINITIONS

---

### General

**Access Code.** A group of readers and time codes assigned to keyholders indicating where and when entry is permitted. Note that access codes can be associated with a down loadable device ID for distributed processing or they can be associated with the host computer for central processing.

**Access Group.** A group of access codes created to facilitate the assignment of similar access privileges to a large number of keyholders.

**Alarm Contact.** A dry-contact switch, indicating input conditions for smoke detectors, heat / moisture sensors, taut-wire fences, window bands, etc.

**Company.** Keyholder's employer.

**Department.** A particular group within a company to which a keyholder is assigned.

**Device.** A controlling element of the system which communicates with the computer and the system points (see *System Hardware* in this section).

**Event.** Any defined transaction which requires action by an access control system. Examples: keyholder entry request, activated alarm.

**Job Category.** A code assigned to a keyholder indicating the employee group category.

**Key Number.** Keyholder's security key number. Unlike the keyholder ID, this number may be changed (e.g., if a key is lost) or removed (e.g., if an employee leaves the company).

**Keyholder.** Employee or visitor who holds a valid security card for an access control system.

---

**Keyholder ID.** Keyholder's ID number. The unique ID number is used by the computer to keep track of all activity for that person. Once entered, the keyholder ID cannot be changed.

**Location.** Location of the office or branch of the company to which a keyholder is assigned.

**Tenant.** One of several distinct occupants of a facility with a single access control system. The data for each tenant using the system appears separate from that of all other tenants.

**Time Code.** A definition of the time of day, and the days of the week, when events are to occur. Used in assigning access privileges, performing scheduled tasks, and monitoring points.

**Trace.** A realtime (as it is happening) display of events for a specific keyholder or point.

**Transactions.** System responses to events are called transactions. The most frequently seen is `ACCESS GRANTED`, which means a valid key was presented to a reader at an approved door, at an approved time, and that the keyholder was granted entry.

**Zones.** Selected locations and device types may be grouped into zones to facilitate system control. For reporting purposes, zones may be grouped into areas. If zones are created, anti-passback instructions or controls may be assigned (see *Access Control Functions* in this section).

## System Hardware — Devices

The principal device is the host computer. The host controls all data maintained in the database, records all system activity, and is the central point for all reporting activity. The host communicates with all system devices, or may communicate via an LC or RLC computer (see *Optional Features* in this section).

Various other devices are included in access control systems. Simple systems may use only contact switches and a single reader type. More complex systems may use several reader types and many other devices. Devices are classified as input or output units depending on their particular function. Input devices are detectors and identifiers; output devices are alarms and control units.

### Devices — Microprocessor Units

**Access Control Units (ACUs).** In conjunction with the host or local computer, the ACUs are used to control door access and maintain status. Example ACUs are: WSE NexSentry, 422, 708P, and 8xx-series. The WSE 708P units are called simple devices because they do not make access decisions (decisions are made by host). The NexSentry, 422, and 8xx-series units are called intelligent devices because they can make access decisions independent of the host.

**Biometric Hand Readers.** Devices such as fingerprint analyzers, hand geometry analyzers, retina scanners, and other devices which check body characteristics.

---

## Readers

**Digital Key Reader.** Reads the unique number of 1 to 5 digital command keys simultaneously at a range of up to 36 inches.

**Keypad Controllers.** The keypad controllers, normally used in conjunction with an ACU, provide additional security by requiring a personal identification number (PIN) entry.

**Magnetic Card Readers.** Reads the card number from information coded into the magnetic strip on the card. Card must be moved physically through the reader to work.

**Readers** (also called Sensors). These units electronically read the security key presented and transmit the data to the ACU. Three reader types are used: Proximity; Magnetic Stripe; Wiegand.

## Inputs

**Alarm Contacts.** These devices monitor simple contact inputs, and control outputs and switches with contact closures for alarm monitoring, elevator control, camera switching, and other tasks.

**Contact Alarms.** Simple dry-contact switches indicating if a contact is open or closed.

**Door switches.** The computer controls only the lock power to the door, and the door switches are the contact points which inform the computer whether a specific door is open or closed. Each door switch is assigned to a specific reader.

**Fire Alarms / Heat Sensors.** Data from smoke detectors and heat sensors can be sent to the computer to alert it to alarm conditions. Although fire alarm systems are generally separate from access control systems, the computer can be used to provide enhanced response capabilities.

**Intrusion Devices.** Taut wire fence, infrared detectors, field-disturbance detectors and other device types can alert the computer to the presence of personnel in unauthorized areas.

**Motion Sensors.** Detect physical movement in an area. Can be used to tell the computer that someone wants to exit (go through a door from the uncontrolled side), or to protect secure areas.

**Video Monitor Switchers.** The computer routes the signal from a particular video camera to a specific monitor based on conditions in that area. For example, if the computer detects an open rear door, it can display the camera output at that door on the terminal at the security desk.

---

---

**Multiple Switch Monitor (MSM).** The MSM is a four-contact switch box that is connected to a WSE ACU and the MSM provides four contact-closure inputs.

**Points.** A point is any basic element of an access control system, such as a door switch, an alarm contact, an output switch. Point IDs uniquely identify all system elements.

**Request-to-Exit (REX) Sensor.** Used when both entry and exit control is required. REX points, usually push-button devices, motion detectors, or push-bars, tell the computer that someone inside a building wants to exit. The computer needs to know this to unlock the door, or to disregard the door opening as being an alarm event.

## Outputs

**Audible Alarms.** The computer can trigger bells, buzzers and other types of audible alarms.

**Remote Alarms.** The computer can dial police and / or fire departments, or any other agency, as part of an alarm response plan.

## System Software

The system software links all input and output elements. The software collects and reports data from input devices, and controls the output devices based on this information. The software also detects and reports any hardware problems that may occur.

**Complete Portability.** A specific computer type is not required, although Hewlett-Packard computers are preferred because of performance and worldwide service. Application programs run under an SCO / UNIX operating system.

**Installation Flexibility.** The SE 6000 can control many hardware setups, including remote site networks. The system can be programmed to control data flow between central and remote computers to create a large-size security system controlled from a central point.

**Integrated Software Support.** The SE 6000 communicates with a variety of access control and alarm monitoring devices. Currently, the system interfaces with WSE ACUs and their peripheral devices, alarm multiplexers produced by Stellar Systems and Optomux, magnetic stripe readers, CCTV camera switchers made by Burle, Pacom, American Dynamics, and Vicon, Radionics alarm panels, and Recognition Systems hand geometry readers. In addition, the system supports communication with the WSE 8xx-series ACUs over dial-up telephone lines using a remote dial-up interface (RDI) device. The ID-4000 badging system includes options for badge designs on film or on PVC.

**Open System Design.** There are few restrictions on the number of security keys, key readers, or other system elements used with the SE 6000. Increasing system capacity only involves upgrading the computer power by adding more memory or disk space, or installing a faster processor. This means that, as a company grows, it cannot outgrow the SE 6000.

---

**Response Time.** The SE 6000 is capable of fast response times in both single and multiple site configurations. Fast response times are important for security personnel who monitor alarms and are always appreciated by keyholders wishing to enter locked doors.

## Principal System Functions

### Access Control

**Anti-Passback Control.** The SE 6000 has anti-passback features (applies to zones only) to prevent tailgating or unauthorized key use. Anti-passback is possible across multiple access control devices, and can be hard (denies access) or soft (allows access, but displays and logs a message). The software handles vehicle and personal passback separately.

**Automatic Access Control.** Permits employees or visitors with assigned access codes to pass through only those doors assigned to them and only during the proper days and hours.

**Automatic Activate / Deactivate.** Permits the automatic activation of specific output points to control lighting, status indicators, or other electrically controlled functions.

**Automatic Unlock / Lock.** Allows doors to be opened automatically only during specified time periods, then re-locked automatically at a later time.

**Communications Monitor.** Permits security personnel to check all wiring and communications to all hardware elements and displays raw data exchange between the host computer and a connected device.

**Event Monitoring.** Displays events as they occur and monitors the door status and other access points. Allows security personnel to watch events at all doors in the system from one location.

**Flexible Event Handling.** Flexible event handling automatically activates outputs, displays special messages, and enables / disables devices. Anything which can be done manually on the SE 6000 can also be performed automatically using this feature.

**Independent PIN Entry.** Access control can be enhanced using personal identification numbers (PINs). PINs are entered via keypad devices assigned to readers. Also, high-security independent devices (hand geometry readers, e.g.) can identify the user.

**Manual Access Control.** Allows security personnel to manually open any door in response to an access request. May be used with closed-circuit TV to verify and admit people, or to track keyholders who have forgotten their keys. Includes the capability to record keyholder IDs if keys are not available. All manual actions are logged as events.

**Two-Man Rule.** The SE 6000 can be programmed to grant access only after two valid key presentations have been made at the same reader within a predefined period of time.

---

**Multiple Occupancy Feature.** Similar to the two-man rule except that it requires that two keyholders enter and leave a specified zone together; refer to Section 4 for details.

## File Maintenance

To perform its access control functions, the system must know the unique ID numbers of all keyholders and the doors and times they can enter. Further, the SE 6000 maintains other keyholder data to facilitate scheduling and reporting.

The system also needs to know details of the location of input devices and other security hardware. File maintenance functions allow users to enter, modify, or delete employee, company, physical connection and time information, as required.

## Reporting

The SE 6000 produces a comprehensive selection of reports for display at the system terminal or for hard-copy output from the system printer:

**Alarms and Responses.** A history report of alarms which occurred at a specific time and location, and the responses taken by the security staff.

**All Transactions.** A report detailing all system activity. The items reported can be limited to specific information items.

**Database Changes.** A report of database change activity, which includes the name of the operator who made the changes. Note that this requires that the journaling feature be enabled.

**Invalid Access Attempts.** A report detailing events which were not valid accesses during specific time periods at particular doors.

**Keyholder History.** A report of the last twenty uses from a particular keyholder.

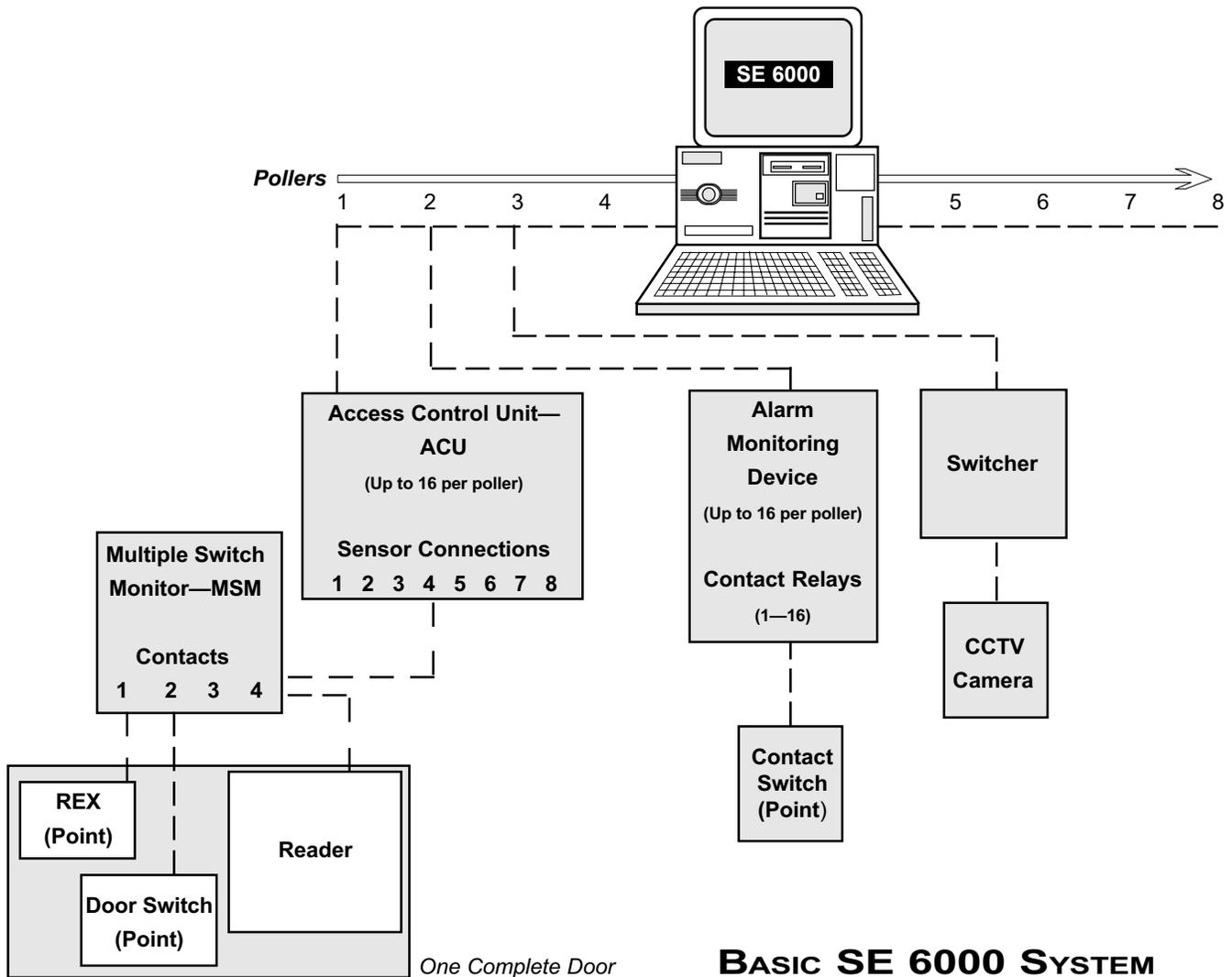
**Point History.** A report of the last twenty events at any door or point. Designed as a quick way to view a limited number of events. Additionally, reports can be created which provide information about the keyholders in the system, access privilege definitions, company information, input devices, and other subjects.

## SAMPLE SYSTEM

---

An illustration of a basic SE 6000 system follows:

---



## CREATING THE DATABASE

Once the system is in place, first obtain the following from the system installer:

**System Interconnect Diagram.** This shows all wiring and connections in the system, and provides information needed for entering pollers, devices, readers, and points.

**Poller Initialization Parameters Information.** The information shows how the pollers were initialized, including poller type, physical port connection, and other poller-specific information. Because all system activity is based on four-digit ID numbers, you need to decide before data entry how these numbers are to be assigned to the system hardware elements. Although the numbering system is entirely the choice of the SE 6000 owner, we recommend one of the two following methods:

1. Following the *System Interconnect Diagram*, number each element in turn with a four-digit number, including numbers for devices, pollers, and readers.
2. Use the following ID groupings for average-sized system:

|           |             |           |                 |
|-----------|-------------|-----------|-----------------|
| 0001-0010 | — Computers | 2000-2999 | — Door switches |
| 0011-0099 | — Pollers   | 3000-3999 | — REX contacts  |
| 0100-0999 | — Devices   | 4000-5999 | — Input points  |
| 1000-1999 | — Sensors   | 6000-7999 | — Outputs       |

## Data Entry Sequence

Note that although the zoom feature (described later in this section) permits faster data entry, WSE recommends the following sequence for most efficient data entry when you are creating your database (data entry is detailed in *Section 4: Master File Entry*):

- |                  |                         |                                       |
|------------------|-------------------------|---------------------------------------|
| 1. Time Codes    | 9. Access Groups        | 17. Tasks                             |
| 2. Tenants       | 10. User-Defined Fields | 18. Events                            |
| 3. Zones / Areas | 11. Keyholders          | 19. Enable Terminals for Global Alert |
| 4. Pollers       | 12. Access Privileges   | 20. Program Security Levels           |
| 5. Devices       | 13. Holidays            | 21. Add Users                         |
| 6. Points        | 14. Alarm Instructions  | 22. Passwords                         |
| 7. Readers       | 15. Maps                | 23. System Owner Name                 |
| 8. Access Codes  | 16. Transactions        | 24. Terminals for Alarm Auto-Switch   |

### NOTE

Consult the system installer if you have questions concerning numbering. In any case, keep track of your numbering method and advise each operator of the method selected

## BASIC SYSTEM USAGE

This subsection gives introductory information for using the SE 6000 system, and includes related miscellaneous information.

### Logging On

Power on the system terminal. The screen displays a brief welcome message followed by the *login* and *password* prompts. Enter the login ID and password in lowercase letters. If uppercase letters are entered by mistake, log off using uppercase letters then log on again with lowercase letters.

If the login and password are not valid or if one or both were not entered correctly, the computer responds with *login incorrect* then displays *login* again. Reenter the login ID and password making sure that each letter is correctly typed. If the *login incorrect* message continues, consult the system administrator. When logged in correctly, the system displays the SE 6000 title page, sets the terminal environment, then displays the main menu. Call WSE Customer Service if you have a login problem.

## System Screens

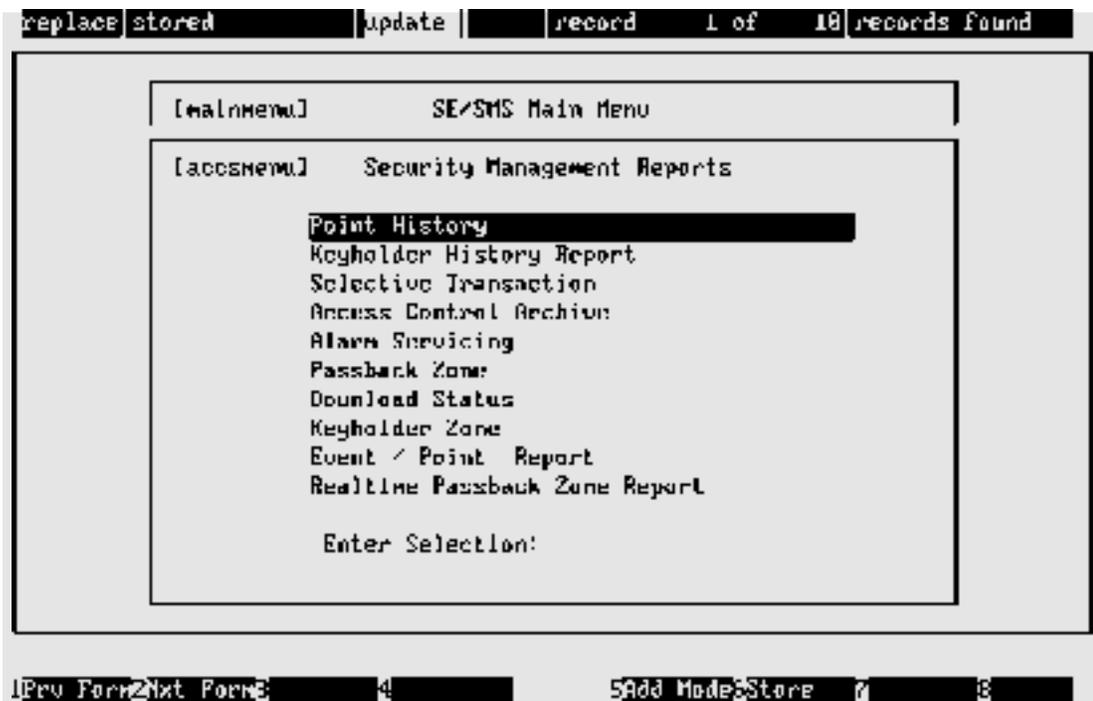
There are two basic screen types: *Menu* and *Application*:

### Menu Screens

Menu screens list application selections by group according to function (exception Monitor Security Activity — see Section 2). All menu screen IDs end in *menu* (example: [fmntmenu] — Master File Entry).

The menu screens have three elements: the list of choices, the highlight bar, and the *Enter Selection* field. The highlight bar, controlled by the arrow keys, is used to make a selection to be placed into the *Enter Selection* field. Screen access descriptions are given in *Moving Between Screens and Fields* in this section.

A sample menu screen follows:



### Application Screens

Application screens use status windows and various fields for entering new data or displaying existing data. The screen title is in brackets and on the same line and to the left of the screen title. Most screen title IDs indicate screen function, e.g., *entr* (enter data), *rprt* (report). A sample screen follows:

```

replace stored/modified update zoom record 1 of 1
[key_entr] Keyholder Entry - Page 1
Keyholder ID: 800012339
Last Name : GOWERS First Name: ERNIE
Key Type: 4 Facility Code: 8000 Key Number: 1447 PIN #: 1221

Tenant Number:4 - GROVE ELECTRONICS, INTERNL
Company :5 = TECHNICAL PUBLICATIONS
Dept :2 = SOFTWARE ENGINEERING
Location :4 = CAMPBELL, CAL.
Job Cal :1 = SALARIED EMPLOYEE
Shift :1 = 8888 1700
Status :1 = FT EXEMPT
Issue Date : 07/12/94 Issue Time: 13:07
Return Date : xxxxxxxx Return Time: xxxxx
Visitor: N Trace: N Privileged: Y
Personal Zone : -1 = UNKNOWN ZONE STATUS (FORGIVEN)
Vehicular Zone: -1 = UNKNOWN ZONE STATUS (FORGIVEN)
Badge Id: 9 = NO BADGE DEFINED
PRESS <F2> <NEXT FORM> AT ANY TIME FOR PAGE 2 OR TO ASSIGN ACCESS

Enter the Badge Id that should be used for this keyholder
IPrv Form2Nxt Form3 4Find Mode 5Add Mode6Store 7Zoom 8

```

Indicates *replace* or *insert* mode. With *replace*, entries overwrite existing data. With *insert*, entries push existing data to the right. Toggle between the modes by pressing *insert*.

Indicates if the information displaying is stored.

Indicates the current screen mode (see *Finding, Adding, and Storing Data* in this section). In some systems, this window is in reverse video.

Indicates if the zoom feature exists for a field (see *Zoom Feature* in this section).

Displays the number of records found as a result of a *find* request (see *Finding, Adding, and Storing Data* in this section).

## SCREEN EXAMPLES

SE 6000 screen displays show the path used to access the screen. For example, the final screen used when setting up keyholders, [epj\_entr], is accessed via three preceding keyholder setup screens: [key\_entr], [key1entr], [empgentr]. This useful feature considerably assists the new SE 6000 user when becoming familiar with the system. A sample [epj\_entr] screen follows:

```

replace not stored | update | zoom | record 1 of 1
[Key_entrl]          Keyholder Entry Page 1
Keyholder ID: 000027793
Last Name : LUCET           First Name: ELISE

[keylentr]          Keyholder Entry - Page 2
Keyholder Id: 27793        LUCET           ELISE

[empgentrl]        Key Holder Access Entry

Access Code Ac | [epj_entrl]          Project Assignment | Access
1 HO | Project Project Description | Override
      | 3 EMERGENCY CIRCUIT BOARD REVISION PROJECT | 0
PRESS < | | HOLDER
Enter a project identification.
1Prev Form2Nxt Form3 | 4Find Mode | 5Add Mode6Store | 7Zoom | 8

```

## USING SCREENS AND FIELDS

### Selecting Screens

There are three screen selection methods:

1. Use the arrow keys to select the menu choice. Press Enter to place it in the *Enter Selection* field, and press Enter again to display the selection.
2. Use the arrow keys to select the menu choice, and press F2 to display the selection.
3. Press Enter anywhere in the list of choices to move the highlight bar to the *Enter Selection* field. Press Ctrl + y to clear the field and type the title of the screen required and then press Enter.

### Moving Between Data Fields

Move between the application screen data fields as follows:

- To move forward through the fields, press Enter.
- To move backward through the fields, press Ctrl + u.
- To move between characters within a single field, use the left and right arrow keys.

---

## Moving to Prior Screens

Press F1 to return to the previous screen displayed. If required, continue to press F1 to return to the system main menu.

---

## FINDING, ADDING, AND STORING DATA

---

### Finding Data

Use the find mode to locate and select data. A specific record (a single keyholder ID, for example) or a group of records (all keyholders in a particular job category, for example) can be found.

For example, assume we need to find all keyholders assigned to tenant 2 who began work after May 1, 1995. First, select the keyholder entry screen, [key\_entr]:

#### NOTE

The *keyholders* are the object of the search, which is why we begin at the keyholder entry screen. *Tenant 2* and *issue date* are the search criteria.

1. Press F4 to clear fields and to enter the find mode. The third status field at the top of the screen displays *find*.
2. Press Enter to advance the highlight bar until you reach the first search item, *Tenant*, and type 2.
3. Press Enter to advance the highlight bar until you reach the second search item, *Issue Date*, and type 05/01/96. (Note: Enter the date according to the format for your system, that is, either MM/DD/YY or DD/MM/YY.)
4. Press F3 to begin the search process; the sixth status field displays *finding*. The length of the search process will depend upon the size of the data base.
5. When the search completes, the system displays the first record found and shows the number of records found in the fifth status window (*Record 1 of n*). (If the system doesn't find any records matching the search criteria, the message *No Records Found* displays.)

Use the down arrow key to display other records found in the search process. Use the up arrow key to go back to previous records.

### Searching With Partial Information

Records can be found using partial information. For example, to find all keyholders whose last name begins with T, enter T in the *Last Name* field. The system also searches for several criteria. For example, to find all keyholders who work for tenants 1 and 5, enter 1,5 in the *tenant* field. In addition, you can enter less than (<) and greater than (>) symbols to narrow a search.

---

The computer automatically changes to the update mode when a search completes, and the records selected can be updated if required. To start another search, press F4 to clear the screen and begin again.

## Adding / Changing Data

The add mode is used to input new records. Once a record is found using the search mode, update is automatically selected which allows the user to change the existing data.

If not already in the add mode, press F5 to clear fields and to begin adding. Press Enter to move the highlight bar to the next field and type the data. (If a typing mistake is made, press Ctrl + y to clear a field, Ctrl + f to delete characters in a field, Ctrl + u to move back through the fields.)

Many fields have default values, which are used if a field entry is not made. Default values are used to simplify the entry process by automatically setting certain fields to commonly used values. For example, many yes or no type fields, (Y / N), have Y as the default.

## Storing Data

Store all additions and changes when completed—Press F6. If F1 is used to return to the previous screen without first storing the new / changed information, all the new data is lost.

---

## DELETING RECORDS

---

From time to time, it may be necessary to delete records from the database. The delete record function is easy to perform, although some cautions are involved. To remove a record from the database, first display the record using the find mode, then press Esc, followed by *d* (lowercase), then *r* (lowercase). If the operation can be performed, the computer displays *deleted*.

It may not be possible to delete records in some cases. For example, the system would not allow a reader to be deleted without first deleting its associated access codes. Display the access code records and delete the reader data appearing on them, then delete the reader record itself again.

### CAUTION

Be careful when deleting certain records. For example, it is unwise to be hasty when deleting keyholder records. Consider Employee A who occasionally entered a certain room where valuable material is stored. The employee then abruptly left the company, and the keyholder record is deleted. A theft is then discovered from the room, and from shipping and receiving records it is determined that the theft occurred within a particular time frame. But with the keyholder information now erased for Employee A, there is no way to link the transaction history to a particular keyholder.

---

---

## ZOOM FEATURE

---

The *zoom* feature provides a fast method for accessing linked or dependent application screens and for copying data from these screens to other application screens. When the feature is available, *zoom* displays in the status bar.

For example, you are entering keyholder data (keyholder entry screen) but don't know the tenant code for the keyholder. When in the *tenant* field, press F7 to *zoom* to the tenant entry screen. Once there, use the find mode to see the tenant codes defined and to select the one you need or enter a new one. Then press F1, and the system automatically returns you to the keyholder entry screen and enters the keyholder's tenant code in the *tenant* field.

### Cancel Zoom

If you don't need data from the *zoom* screen, press *Esc*, then Ctrl + z to return to the previous screen, or simply return using F1 and key over the returned data.

---

## MISCELLANEOUS INFORMATION

---

- If you need help in any field in the system, check the instructions on the information line at the bottom of the screen.
- If the computer beeps and displays a message, or if you see the symbol '---' in the information area at the bottom of the screen, press Enter to let the computer know you've read the message. The computer will not allow further action, and will beep each time you press a key until you press Enter to acknowledge.
- Occasionally, a screen will not display properly. This can occur when accessing the system from a remote dial-in terminal via a modem or when the system administrator sends a message. If this happens, try using Ctrl + r to redraw the screen. To completely clear the problem, log off the system and log on again.
- To save time when moving around the SE 6000 system, it pays to learn the screen titles of the most commonly used application screens (see the screen location trees and the table at the end of this section). For fast screen access, type a screen title in the *Enter Selection* field (press Enter in any menu screen), then press Enter and the system immediately displays the screen. Note that you should delete any characters remaining in the *Enter Selection* field before you select Enter.

---

## LOGGING OFF

---

When the SE 6000 session is completed, press F1 until you reach the main menu screen. From here, press F1 again; the computer asks for log off confirmation. Enter yes (full word) and press Enter to leave the system. (You can also type exit in any Enter Selection field to leave the system.) After log off, the computer displays the login prompt again.

---

**IMPORTANT**

Log off the SE 6000 system formally before you leave the terminal. If you do not log off, any action taken by the next person at the terminal will appear under your name.

---

**SHUTTING DOWN**

---

Always use the following procedures, in the order given, when powering off the SE 6000:

1. Go to the main system terminal (system console). This terminal has overall computer control and displays all system messages.
2. Log off the system using the procedures given in the previous subsection.
3. Log in using the SHUTDOWN login. Your system administrator will provide you with the password. If other users are still logged on, you may have to press Enter to continue the shut down process which will forcibly log off other users.

Step 3 automatically shuts down the SE 6000 system in an orderly way. The last message displayed when the internal shutdown procedures have completed is *Safe to Power Off or Press any Key to Reboot*. It is now safe to power off the computer. To restart the computer, press any key and follow the instructions in the following subsection.

---

**RESTARTING**

---

Use one of the following methods, *Automatic* or *Manual*, when powering on the SE 6000 (the shutdown / restart process is also known as *rebooting* the computer).

**Automatic Restart**

The SE 6000 has an automatic restart capability that reboots the system in the event of a power interruption. If unattended, the *Boot* prompt displays for 30 seconds, then the auto-boot function reloads the operating system and restarts the application including the pollers.

**Manual Restart**

1. Turn the power on; the computer displays *Boot*. Press Enter to continue.
  2. After various messages, the computer displays *Type Control-d to Proceed with Normal Startup (or give root password for system maintenance)*. Press and hold the Ctrl key, and press the *d* key (lowercase).
-

3. The computer displays *Enter new time ([yyymmdd]hhmm)*. Change the date and time values as required (do not enter the parentheses or brackets); press Enter when completed. To keep the displayed date and time, press Enter.
4. The computer continues its startup procedures, and the *login* prompt displays after a brief pause. If any other message displays apart from those noted here, just press Enter.

---

## SYSTEM SCREEN TREES

---

The SE 6000 screens are arranged in tree structures, with hierarchies established from the primary screen to the lowest level screens in each tree. Each screen has a unique title which displays in the upper-left.

### Appendix A: System Screen Trees

Tree structures for the first seven standard-product selections on the system main menu are given in *Appendix A*:

- Monitor Security Activity
- Security Management Reports
- Master File Entry
- Master File Reports
- Key Inventory / Parking Stickers
- System Administration

### Appendix B: System Screen Hierarchies

*Appendix B* lists all screens within their respective tree structures, along with a brief explanation for each. Left column indentions show the relative position of each screen within the individual tree structures. Indented screens can be accessed only from the previous level in the screen hierarchy.

---

## OPTIONAL FEATURES

---

A variety of optional software packages are available with the SE 6000:

***IQ.*** A report writer package that allows the user to select, sort, display and / or print database information in a format specified by the user. It can be used for quick ad hoc enquiries or formal reports. Once defined, report formats may be saved and rerun on demand.

***CCTV Camera Switcher Control.*** Controls the actions of closed-circuit television system switchers, allowing the system to switch video output from a particular camera to a specified monitor. When used in conjunction with the system flexible event handling feature, this provides an important method for monitoring system events.

---

**Controller Systems.** Controller systems are computers running the SE 6000 local (LC) or remote location controller (RLC) software. The LC system is a computer attached via dedicated lines to the host. The RLC system is a computer attached via dial-up telephone lines to the host.

**Elevator Control.** Permits floor-by-floor control of elevator call buttons. When a keyholder presents a key to a reader in the elevator, certain buttons, wired via computer-controlled output contracts, can be enabled or disabled for use. The keyholder is able to select only those which have been enabled for his / her specific access privileges.

**Guard Tour.** Schedules and monitors security personnel guard tour activities. Specifies certain reader output points as guard tour points, and assigns the minimum and maximum times which can pass between stops on the tour. The feature reports if tours have started too early or too late, or if too little or too much time has passed between stations.

**Parking Control.** Controls and monitors a parking facility including employee and revenue generating parking spaces. Includes keyholder and daily cash customer functions, tenant billing, and overage features. Supported hardware includes point-of-sale terminals, automated ticket dispensers, and gate control mechanisms. Produces detailed reports for keyholders, cash customers, parking lot attendant activity, and keeps track of the number of cars in the lot on a tenant-by-tenant basis.

**Remote Dial-Up Interface (RDI).** Permits communication with remotely-located 8xx-series devices via dial-up telephone lines. The feature retains transaction information, and determines when conditions at a remote site warrant a call to the host (alarm event occurring, log buffer reaching a user-defined threshold, etc.). Frequency and call duration are determined by the user. The host contacts remote sites in turn to access information and to transfer event logs.

**Time and Attendance.** Captures hours worked by each employee for transfer to a payroll or accounting system. The feature can be programmed to:

- Generate specialized reports of time and attendance activity.
- Monitor the number of meals taken by a keyholder.
- Recognize early and late entrances and exits.
- All records can be edited and modified prior to transfer to another system.

**Visitor Control.** Tracks visitors, prints visitor badges (black and white or color), and creates comprehensive reports of visitor activity. The feature also provides a record of who was visited and the date. It provides the company name of the visitor if applicable.

**WSEID-4000 Interface.** Integrates one or more Polaroid ID-4000 photobadging systems with the SE 6000. Keyholder information and photo IDs created on the Polaroid system are transferred via a LAN or serial connection to the SE 6000. Badges can be printed on film or on PVC. Keyholder maintenance may be initiated on either system; all data is stored in a single database resident on the SE 6000.

---



## FUNCTION KEYS

Beneath the transactions display are the applicable function keys for each screen, with the key actions shown next to the key numbers. For most function key actions, the system displays messages confirming that the action has been completed, e.g., POLLER STOPPED.

In general, F1 is used to exit from the current screen, and F7 and F8 are used respectively to display the previous screen and the next screen within the set of screens that apply to the particular data item being controlled or when there are more items than will fit into a single screen.

## DATA ITEM SELECTION

Use the up and down arrow keys to select the data item to be controlled, then press the applicable function key for the system action to be taken.

## CONTROL FUNCTIONS MENU

### Pollers

The Control Pollers screen displays point ID, description, status.

```
[Monitor] Mon Jun 17 11:48 [COMLEY.ROM ] ALARMS PND:1 ACT:0
Control Pollers
```

| PntId | Description        | Status    |
|-------|--------------------|-----------|
| 0002  | HOST/LC POLLER     | ONLINE    |
| 0010  | HOST 70BP POLLER   | ONLINE    |
| 0050  | BAILC1 P1 70BP     | ONLINE    |
| 2001  | HCC1 POLLER 2      | ONLINE    |
| 2201  | RD1 SCHED/DIALER   | ONLINE    |
| 2999  | LAWRENCE P1 70BP   | ONLINE    |
| 3000  | LAWRENCE P2 80BP   | ONLINE    |
| 4000  | HOST OPTO POLLER 4 | ????????? |

### Control Pollers Function Keys

**F2 HALT.** Stop a poller when work is to be performed on devices attached to the poller or to reload a poller parameter following a change.

**F3 RESTART.** Restart the poller when work is completed (system displays messages announcing each device attached to the poller as it comes back online). If there are devices with system or key checksum errors, perform a reset to the device.

**F4 DEV COMM.** This function monitors communication between the pollers and the device pollers. In normal operation, the devices are asked for information by the pollers many times a second, and with a properly operating system the controller screen updates rapidly.

When F4 is pressed, a second screen displays showing the connections between the host and the devices of the particular poller selected:

```
[monitor] Mon Jun 17 11:49 [CONLEY.ROM ] ALARMS PND:1 ACT:0
Control Pollers
Device Poll Msg Response Data Request Response Command Response
1 P0X28 M0F00DD
2 P1X27 M1F00DC
3 P2X26 M2F00DB
4 P3X25
```

Poller-device communication should be one of the first items checked whenever there is an apparent problem with the system.

## Devices

The Control Devices screen displays point ID, description, status, tamper, shunt. Applies to NexSentry, 422, and 8xx-series ACUs.

```
[monitor] Mon Jun 17 11:49 [CONLEY.ROM ] ALARMS PND:1 ACT:0
Control Devices
Pntid Description Status Tamper? Shunt
0001 BA1 HOST ONLINE NORMAL
0003 P1 700P DEV 2 ONLINE FAIL
0004 P1 700P DEV 3 ONLINE FAIL
0005 7024 NUMBER 4 ONLINE NORMAL
0051 BA11C1 P1 DEV 1 ONLINE NORMAL
0052 BA11C1 CONTROLLER ?????????? NORMAL
0050 LAWRENCE CONTROLLER ONLINE NORMAL
0061 LAWRENCE P2 800S 1 ONLINE FAIL
```

## Control Devices Function Keys

**F2 DEV STAT.** Device Status—When F2 is pressed, a second screen displays showing the status of the particular device selected:

```
[monitor] Mon Jun 17 11:49 [CONLEY.ROM ] ALARMS PND:1 ACT:0
Control Devices
Pol Addr Status LockStat D R Msmstats
01 02 ONL.TMR
LOCK N N N N N N
LOCK N Y N N N N
LOCK N M N N N N
LOCK N N N N N N
LOCK N M N N N N
```

**F3 DEV RSET.** Device Reset—Used when setting up new ACUs or reestablishing repaired ACUs, or when the integrity of the data currently resident in the ACU is suspected. Downloads all host device data to the ACU and silences a latched alarm.

**F4 KEY RSET.** Key Reset—Used when setting up new ACUs or reestablishing repaired ACUs, or when the integrity of the data currently resident in the ACU is suspected. Downloads all host key data to the ACU.

**F5 SHUNT.** Shunt a device.

**F6 UNSHUNT.** Unshunt a device previously shunted.

## Locks

The Control Locks screen displays point ID, description, lock status, shunt, sensor, coax, door status.

```

[monitor] Tue Mar 30 16:53 [No Enplid Re ]           ALARMS PND:1 ACT:0
ALL ENCOMPASSING           Control Locks
PntId Description          Lck Stat Shunt Sensor Coax Door Stat
0121 P1 D2 R3 (ZONE 45)    ???????             NORMAL  NORMAL  N/A
0122 P1 D2 R2 (ZONE 1)    ???????             NORMAL  NORMAL  ???????
1111 P1 D1 R1              ???????             NORMAL  NORMAL  N/A
1112 P1 D1 R3              ???????             NORMAL  NORMAL  N/A
1113 P1 D1 R7              ???????             NORMAL  NORMAL  N/A
3110 8085X RDR 1           LOCK                 FAIL    NORMAL  N/A
3120 8085X RDR 2           LOCK                 NORMAL  NORMAL  N/A
3170 8085X RDR 7           LOCK                 NORMAL  NORMAL  N/A

```

## Control Locks Function Keys

**F2 LOCK.** Lock selected door. If no door is selected, F2 locks all doors in the zone.

**F3 UNLOCK.** Unlock selected door. If no door is selected, F3 unlocks all doors in the zone.

**F4 TIME OPEN.** Unlock selected door for the amount of time programmed at the ACU or on the reader entry screen. If no door is selected in a zone, F4 unlocks all doors in the zone for the amount of time programmed.

**F5 SHUNT.** Shunt a door.

**F6 UNSHUNT.** Unshunt a door previously shunted.

## Input Points

The Control Inputs screen displays point ID, description, point status, tamper, shunt.

```
[monitor] Mon Jun 17 11:52 [COMLEY.ROM ] ALARMS PND:1 ACT:0
Control Inputs
PntId Description Pnt Stat Tamper Shunt
0068 I.C.U. PUSH BAR GPS3 NORMAL NORMAL
0069 I.C.U. LIGHTS GPS4 NORMAL NORMAL
0072 ANIMAL LAB GPS3 NORMAL NORMAL
0073 ANIMAL LAB GPS4 NORMAL NORMAL
0103 S.E. GARAGE SPITTER NORMAL NORMAL
0104 N.W. GARAGE SPITTER NORMAL NORMAL
```

## Control Inputs Function Keys

**F5 SHUNT.** Shunt a selected input point. If no input point is selected, F5 shunts all input points in the zone.

**F6 UNSHUNT.** Unshunt a selected input point previously shunted. If no input point is selected, F6 unshunts all input points in the zone.

## Output Points

The Control Outputs screen displays point ID, description, status, shunt.

```
[monitor] Mon Jun 17 11:52 [COMLEY.ROM ] ALARMS PND:1 ACT:0
Control Outputs
PntId Description Status Shunt
4103 PARKING LOT LIGHTS NORMAL
4104 SURVEILLANCE CAMERAS ACTIVE
4203 HALLOW COMPUTER ROOM NORMAL
4204 WATER SPRINKLERS NORMAL MAN SHUNT
```

## Control Outputs Function Keys

**F2 ACTIVATE.** Activate a selected output point. If no output point is selected, F2 shunts all output points in the zone.

**F3 NORMAL.** Deactivate a selected output point. If no output point is selected, F3 deactivates all output points in the zone.

**F5 SHUNT.** Shunt a selected output point. If no output point is selected, F5 shunts all output points in the zone.

**F6 UNSHUNT.** Unshunt a selected output point previously shunted. If no output point is selected, F6 unshunts all output points in the zone.

## Doors

The Control Doors screen displays point ID, description, status, and shunt of the door switches.

```
[monitor] Mon Jun 17 11:52 [CONLEY.ROM ]           ALARMS PND:1 ACT:0
Control Doors
PntId Description      Status  Shunt
0066 INTENSIVE CARE DS  CLOSED
0070 ANIMAL LAB DS     CLOSED
0101 DINING HALL DS    CLOSED
0201 CHEMICALS DS     CLOSED
1011 DGE DS            CLOSED  TIM SHNT
1001 CONTROLL. GATE DS  CLOSED
```

## Control Doors Function Keys

**F5 SHUNT.** Shunt a selected door. If no door is selected, F5 shunts all doors in the zone.

**F6 UNSHUNT.** Unshunt a selected door previously shunted. If no door is selected, F6 unshunts all doors in the zone.

## Select Zone

The Select Zone screen displays zone, description, count, PBarea, PBtype, PBlevel (see **F3 RSET CNT** below).

```
[monitor] Fri Mar 10 10:33 [ADMIN.SVS ]           No Alarms Pending
ALL ENCOMPASSING
Select Zone
Zone Description      Count  PBarea  PBtype  PBlevel
0 ALL ENCOMPASSING    1
1 ALPHA LAB ZONE      0      PERSONAL  HARD    GLOBAL
2 HARD PASSBACK TEST ZONE 2  0      PERSONAL  HARD    LOCAL
3 HARD PASSBACK TEST ZONE 3  0      PERSONAL  HARD    LOCAL
4 HARD ANTI PASSBACK TEST  0      VEHICLE   HARD    GLOBAL
5 HARD PASSBACK TEST ZONE  0      VEHICLE   HARD    GLOBAL
6 GREEN ZONE NORTH     0      PERSONAL  SOFT    GLOBAL
7 FRONT ENTRANCES - MAIN  0      PERSONAL  SOFT    GLOBAL
```

Use the arrow key to make the desired selection and press F2. Control activity remains exclusively for this zone until you return to the monitor menu.

The keyholder count fields apply if passback control is in effect for the zone selected

## Select Zone Function Keys

**F2 SEL ZONE.** Select zone.

**F3 RSET CNT.** If passback control is in effect for a zone, the following display:

- Count** — Number of keyholders currently in the zone.  
**PBarea** — Passback zone type—personal, vehicle, none.  
**PBtype** — Passback type—hard, soft, none.  
**PBlevel** — Passback control—global (host), local (ACU), none.

Note that zone count is automatically reset whenever a zone is selected.

Multi-user systems employ record locking techniques for keyholder file maintenance, and locked records are not updated by the passback routine that maintains keyholder location. If this occurs, the keyholder count is correct, but the passback zone report (which reads the keyholder file) does not include the locked records.

F3 corrects the zone count where privileged keyholders (not subject to passback control) have reentered a controlled zone without having exited in the normal manner or when the previous defined condition exists.

## REVIEW TRANSACTIONS (FULL SCREEN)

This feature displays all transactions in the review transaction memory. Typically, the last 3,000 transactions which occurred are available. To view the screen without interruption, new transactions do not appear when using this function. If no keyboard action is taken with this feature for a five-minute period, the system returns to the monitor menu. A sample full screen follows:

| Top Transaction date/time: Fri Mar 18 07:39:42 1994 |                   |          |          |              |                       |
|---|-------------------|----------|----------|--------------|-----------------------|
| Point   | Location          | Time     | Key      | Name         | Message               |
| 10  | LC #1             | 07:39:42 | 3499630  | HILLBUN, TIM | SHUNT POINT           |
| 7113  | 7114 ALARM ENABLE | 07:40:04 |          |              | INPUT POINT ACTIVE    |
| 7114  | PRIORITY 10 ALARM | 07:40:04 |          |              | PRIORITY 10 ALARM     |
| 7114  | PRIORITY 10 ALARM | 07:40:07 |          |              | ALARM CLEAR           |
| 7113  | 7114 ALARM ENABLE | 07:40:07 |          |              | INPUT POINT NORMAL    |
| 7114  | PRIORITY 10 ALARM | 07:40:24 | 3499630  | HILLBUN, TIM | ALARM ACKNOWLEDGED    |
| 7114  | PRIORITY 10 ALARM | 07:40:24 |          |              | ALARM RESOLVED        |
| 10  | LC #1             | 07:40:34 |          |              | CONTROLLER COMM ERROR |
| 10  | LC #1             | 07:40:57 | 3499630  | HILLBUN, TIM | UNSHUNT POINT         |
| 10  | LC #1             | 07:40:57 | 3499630  | HILLBUN, TIM | UNSHUNT POINT         |
| 10  | LC #1             | 07:41:29 | 3499630  | HILLBUN, TIM | SHUNT POINT           |
| 10  | LC #1             | 07:41:31 | 3499630  | HILLBUN, TIM | UNSHUNT POINT         |
| 2   | DATABASE POLLER   | 07:41:43 | 3499630  | HILLBUN, TIM | POLLER STOPPED        |
| 2   | DATABASE POLLER   | 07:41:44 | 3499630  | HILLBUN, TIM | POLLER STARTED        |
| 10  | LC #1             | 07:40:41 |          |              | HOST COMM. STOPPED    |
| 10  | LC #1             | 07:41:22 |          |              | HOST COMM. STOPPED    |
| 10  | LC #1             | 07:41:43 |          |              | HOST COMM. STARTED    |
| 7100  | 700P PARKING CHLR | 08:22:17 | 99999999 | ADMIN, SVS   | REQUEST RESET KEYS    |
| 810   | ALPHA LAB B10 #7  | 08:53:10 |          |              | USER LOGGED INTO TERM |
| 810   | ALPHA LAB B10 #7  | 08:58:30 |          |              | USER LOGGED OFF TERM  |

1 Prev 2 Backward 3 Forward 4 Oldest 5 Latest 6 7 8

## Review Transactions Function Keys

**F2 BACKWARD.** Page backward through the transactions.

**F3 FORWARD.** Page forward through the transactions.

**F4 OLDEST.** Go to first transaction.

**F5 LATEST.** Go to last transaction.

## ALARM SERVICING

The system emits beeps when an alarm occurs, and displays the number of pending and active alarm data in the upper-right corner of the monitor menu screen: Pending—alarm condition no longer occurring but not yet formally resolved. Active—alarm condition still occurring. Begin resolving alarms using the alarm servicing screen:

| Alarm Servicing - Currently Pending Alarms |    |       |             |          |          | 19/04/94 08:56    |
|--|----|-------|-------------|----------|----------|-------------------|
| Alarm #                                    | lv | Point | Description | Date     | Time     | Tran Description  |
| 2372                                       | 10 | 0124  | BB0SX ALARM | 04/19/94 | 08:56:18 | PRIORITY 10 ALARM |

## Alarm Servicing Function Keys

**F2 VIEW MAP.** Press F2 to display a map showing alarm location. Location indicated by the point ID in a red rectangle (other map symbols do not display when an alarm is triggered).

**F3 INSTRUCT.** Instructions—Press F3 to display a list of actions to take in response to the alarm.

**F4 RESPONSE.** Press F4 to display the alarm response entry screen. First enter Y or N in the situation resolved field (Y cannot be entered if the alarm is still occurring—take action to halt the alarm condition), then enter the actions taken. A printable record of these actions is written to disk (see *Section 3: Alarm Servicing Report*).

**F5 FAST ACK.** Fast Acknowledge—Press F5 and the alarm is considered resolved (use with caution because this does not allow entry of operator response to an alarm).

**F6 SIL ALL.** Silence All—Press F6 to silence beeping at all terminals.

## REAL TIME CONTROL MAPS

System activity can be monitored using the system map function (created using the DRAWMAPS function—see *Section 4: Maps*). The maps display triggered alarms (icon displays in red; goes to yellow when pending), door status (message displays), device shunt status (message displays), door unlocks (icon goes from black to white).

## CONTROL PROJECTS

The Control Projects screen (not controllable on LC systems—host only) displays project, status, description, start, end. The control projects screen permits operator override of doors assigned to projects which directly affects keyholder access.

```
[monitor] Fri Mar 18 12:56 [ADMIN,SYS ]           No Alarms Pending
M.I. ENCOMPASSING           Control Projects
Proj Status:  Description                Start      End
0001 ACTIVE  TEST PROJECT #1                      9311011552 9411011556
0002 INACTIVE TEST PROJECT #2                      9311050700 9311062359
0003 INACTIVE TEST PROJECT 3 - 700 DOORS          9311030000 9311052359
0005 ACTIVE  EMERGENCY CIRCUIT BOARD REVISION PROJECT 9312170000 9311012359
0009 INACTIVE NEW TEST PROJECT                    9311230000 9311252359
5050 INACTIVE LAUNCH                               9402160000 9402201700
8010 INACTIVE TEST PROJECT 4                      9311050000 9311102359
8020 INACTIVE TEST PROJECT #5                    9311100000 9311202358
```

### Control Projects Function Keys

**F2 ACTIVATE.** Activates a project.

**F3 DE-ACTIV.** Deactivates a project.

**F4 NORMAL.** Normalizes a project based on start/stop dates and time.

## ABORT TIMERS

The Abort Timers function (F6) allows you to stop interactive timers that have started.

## OTHER FUNCTIONS

### Printer Control

```
[monitor] Mon Jun 17 12:05 [CONLEY,ROM ]           ALARMS PND: 1 ACT: 0
Activate / Deactivate Log Printers

1) Exit
3) Reload Printer Information
5) Turn On Printer 1
6) Turn On Printer 2
```

### Control Printers Function Keys

**F3 RELOAD.** Reloads printer data from the host which resets the printer logic and font size.

**F5 PRNT ON.** Switch printer #1 on or off depending on current state (used to control log printer only).

**F6 PRNT ON.** Switch printer #2 on or off depending on current state.

## Forgive Passback

A passback violation occurs when a keyholder uses their key to reenter a door without first using their key to exit the same door. For example, a keyholder (number 1) uses their key and unlocks the door. The system flags keyholder number 1 as "in." Keyholder number 1 passes their key to keyholder number 2. When keyholder number 2 attempts to use the key, the systems gives keyholder number 1 a passback violation. This was originally developed for parking lot control. The system handles vehicle and personal passback separately.

To allow the keyholder to enter the area, use the forgive passback function.

1. Enter key number (or ALL for all keyholders); press Enter.
2. Press F1 to confirm the passback forgive.

## Manual Access Granted

Used when a command key is not available (misaid, stolen, etc.), this function allows the operator to grant manual access following entry of the key number (system records entry). Enter the key number and reader ID. Enter the keyholder ID if the key number is unknown. Manual access is available for all keyholders at any reader regardless of access assignments.

## Force Table Download

This function first writes database information to a text file, then transfers the information to host memory and LC memory (if applicable). The function is used during system servicing, and when requested by customer support. A sample screen follows:

```
[monitor] Fri Mar 18 10:44 [ADMIN,SYS ]           No Alarms Pending
          1-Key      12-Zone   22-DrubBB
          2-Point   13-Project 23-Site
          3 Accode  14 PrjRdr  24 ABA
Enter File# (0 for ALL files) :          4-TLwrrd  15-ExpPrj  25-Map
          6-Dlran   16-RptBBB  26-DKR
          7 ExpAc  17 FstL
          8-Event  18-Instr
          9-Task   19-Hold
         10 Dialr  20 Elev
         11-OverC  21-Node
```

When requested, enter the number of the table to be downloaded and press Enter. The system requests confirmation — press F1. REPACK OK displays when transfer completes.

## Remote Devices

This function is used to establish a telephone connection to a remote device to perform certain actions, for example, unlock a door to a remote ATM for Service. Note that the remote device remains connected until the operator selects the device and presses F3-Hang Up.

```
[Monitor] Wed Oct 14 15:17 [No Emplid Re ]          ALARMS PND: 2 ACT: 0
Control Remote
Pntid Description      Status  Shunt  Last called  Fail
3800 P11 SE422 (DIAL UP) ?????????? 12/31/89 19:00 1
5000 ALC DEVICE        ?????????? MAN SHNT 09/11/92 14:34 H 1
7001 RD1 1 TD TOP 000  ?????????? 10/08/92 16:48 H 0
```

## Control Remote Devices Function Keys

**F2 CALL/HLD.** Call device.

**F3 HANGUP.** Disengage connection.

## Building Modes

Building modes — open, closed, limited — combined with the ACU report definitions provide an extra level of security when the building is empty or a reduced number of staff are present. Door switches and / or other monitor points active in the building open mode can be configured to generate alarms if activated when the building is in limited or closed mode. Also, if open mode, closed mode, or station readers have been defined, reader operation for those locations will change when the building mode changes. For example, an open mode reader will not read keys when the building is in limited or closed mode.

```
[Monitor] Fri Mar 10 10:47 [ADMIN.SYS ]          No Alarms Pending
Control Building Modes
Pntid Description      ACU Status  Building Mode
0021 LC #11 REMOTE 422 1  ??????????  CLOSED
0100 DIAL-UP 422 #1     ??????????  CLOSED
0001 TIM'S BOSSX #2    ONLINE     OPEN
0002 TIM'S BOSS #1    ONLINE     OPEN
0003 ALPHA LAB BOSSX #10 OFFLINE    OPEN
```

## Control Building Modes Function Keys

**F2 OPEN.** Change current building mode to open.

**F3 LIMITED.** Change current building mode to limited.

**F4 CLOSED.** Change current building mode to closed (takes approximately one minute to complete). If a device input point configured to prevent building closure is active, the building will remain in the limited mode until the point is cleared.

## Full Screen Monitoring

Displays system logs in a manner similar to the review transactions feature (see *Review Transactions—Full Screen* in this section) except that new transactions display as they occur. Use F8 to toggle between full and half screen displays.

## MISCELLANEOUS INFORMATION

### Disk Almost Full Warning

This feature warns operators when the disk drive has reached a specified percentage of its total capacity:

| Top Transaction date/time: Thu Mar 17 14:31:29 1994 |          |          |     |      |                  |
|---|----------|----------|-----|------|------------------|
| Point   | Location | Time     | Key | Name | Message          |
| 1   | HOST     | 14:31:29 |     |      | DISK ALMOST FULL |

When the warning appears, take immediate action to reduce the amount of data stored on the disk (delete unwanted files, etc.).

This feature uses the DISKWARN keyword parameter located in the \$DATAPATH/PARAMS.M file:

| Parameter                | Default Condition                             |
|--------------------------|---|
| DISKWARN keyword missing | — Defaults to 90%                             |
| DISKWARN =0              | — Feature disabled                            |
| DISKWARN = <i>n</i>      | — Feature enabled; <i>n</i> is the range 1—99 |

#### NOTE

1. Shut down and reboot after changing DISKWARN parameters.
2. The DISK ALMOST FULL message is generated only once.
3. Since the message is generated only once, we recommend that system message #242 be changed to an alarm event by changing the alarm priority field to a value greater than 0. See *Section 6, Transactions [tranentr]* for details.

## Status Screen Function Timeout

Some system functions temporarily disable the realtime display until the sub-menu is exited. The status screen function Timeout feature provides a user-defined method for controlling the length of time that the realtime display is disabled. If the system does not detect any keyboard or mouse activity for the number of seconds defined by the TIMEOUT parameter, the monitor program returns to the previous menu and resumes realtime display.

This feature uses the parameter file \$DATAPATH/MONITOR, with the control parameter TIMEOUT having a numeric value in seconds:

| Parameter         | Default Condition  |
|-------------------|--|
| Parameter missing | — TIMEOUT defaults to 0—feature disabled                                 |
| TIMEOUT=0         | — Feature disabled   |
| TIMEOUT= <i>n</i> | — Feature enabled using the numeric value <i>n</i> (five digits maximum) |
| TIMEOUT=600       | — Feature enabled using the numeric value 600—600 seconds, default       |

### NOTE

1. The control parameter is read by the monitor program at log-on time and remains in effect as long as the monitor program is active. A change to the Timeout value does not take effect until the user logs off, and then logs back on to the system (reboot not required).
2. This feature is operational with the following screens:
  - A. The device communication function of the control pollers screen (see *Pollers* in this section).
  - B. The device status function of the control devices screen (see *Devices* in this section).

## Alarm Servicing — No Activity Timeout

This feature controls how long the alarm servicing screen displays when there is no keyboard or mouse activity. On Timeout, the system exits the alarm servicing program and returns to the realtime display of system events.

This feature uses the \$DATAPATH/ALARMSRV parameter file, with the control parameter TIMEOUT having a numeric value in seconds: Acceptable values are:

| Parameter         | Default Condition  |
|-------------------|--|
| Parameter missing | — TIMEOUT defaults to 0—feature disabled                                 |
| TIMEOUT=0         | — Feature disabled   |
| TIMEOUT= <i>n</i> | — Feature enabled using the numeric value <i>n</i> (five digits maximum) |
| TIMEOUT=600       | — Feature enabled using the numeric value 600—600 seconds, default       |

**NOTE**

1. The control parameter is read by the alarm servicing program at log-on time and remains in effect as long as the alarm program is active. A change to the Timeout value does not take effect until the user logs off, and then logs back on to the system (reboots).
2. Timeout is deactivated when responding to an alarm in the alarm response screen.

## Monitoring Security - Passwords

With enhanced monitor security function and the addition of password logic, any or all portions of the monitor functions can be set up to require a valid ID and password combination before the function can be initiated. In place of the factory-supplied status login, the user may create a similar login ID, with or without password, and control access to monitor capabilities. While many operators may use the generic login, individual users will have only monitor privileges consistent with their own custom security profiles.

This feature uses the PASSWORD keyword parameter located in the \$DATAPATH/MONITOR file. The acceptable values are:

|                          |   |                            |
|--------------------------|---|----------------------------|
| PASSWORD keyword missing | — | Feature disabled           |
| PASSWORD=0               | — | Feature disabled (default) |
| PASSWORD=1               | — | Feature enabled            |

This feature also requires that the user has a custom security profile. See also note #1 regarding system upgrades with users created on an earlier version of the software.

## Implementing the Feature

For additional information see Chapter 6, Adding a User.

1. Log on using an assigned login name and password, or use a generic login name (and optional password) as required by facility procedures.
  2. With the password feature enabled, any action attempted from the monitor for which permission has not been granted causes the system to prompt for a login name and password.
  3. If the login name and password entered are valid, the associated security profile initiates the action requested (see note #4).
  4. If the feature is disabled or an incorrect login / password is entered, the system displays PERMISSION DENIED.
-

**NOTE**

1. If your system has been upgraded, and users created on a previous release have been saved, their user profiles must be updated with the new monitor security privileges. To do this, log on as addusers with the correct password, select system administration, and then select add users. Update the security profile for each user as follows:
  - Enter the user ID
  - Select modify—F5
  - Press the return key through all fields
  - Store the updated profile—F8

Repeat for all applicable users. The new custom security information is appended without changing the current privileges.
2. If the password keyword parameter is changed, users must log off then log back on (reboot) before a change is recognized by the monitor program.
3. All functions that generate log messages are logged with the user ID entered to gain access to the requested function.
4. Permissions associated with the entered login ID remain in effect until the operator returns to the point where the login ID and password were required, or, if the status screen function Timeout feature has been enabled, the screen itself will Timeout (see *Status Screen Function Timeout Feature* in this section).

## Modified Usage of Invalid Facility Code Log

This feature suppresses a keyholder's name from the monitoring screen and various reports when an INVALID FACILITY CODE message is logged. In some cases, this resulted in a log message erroneously associating a valid keyholder with an invalid facility. This function is automatic and does not require operator action.

**NOTE**

This occurred with the 708 type device where different facility codes were used on different buildings. It only applies to 1030/1040 cards with facility codes where a user has keys with multiple codes.

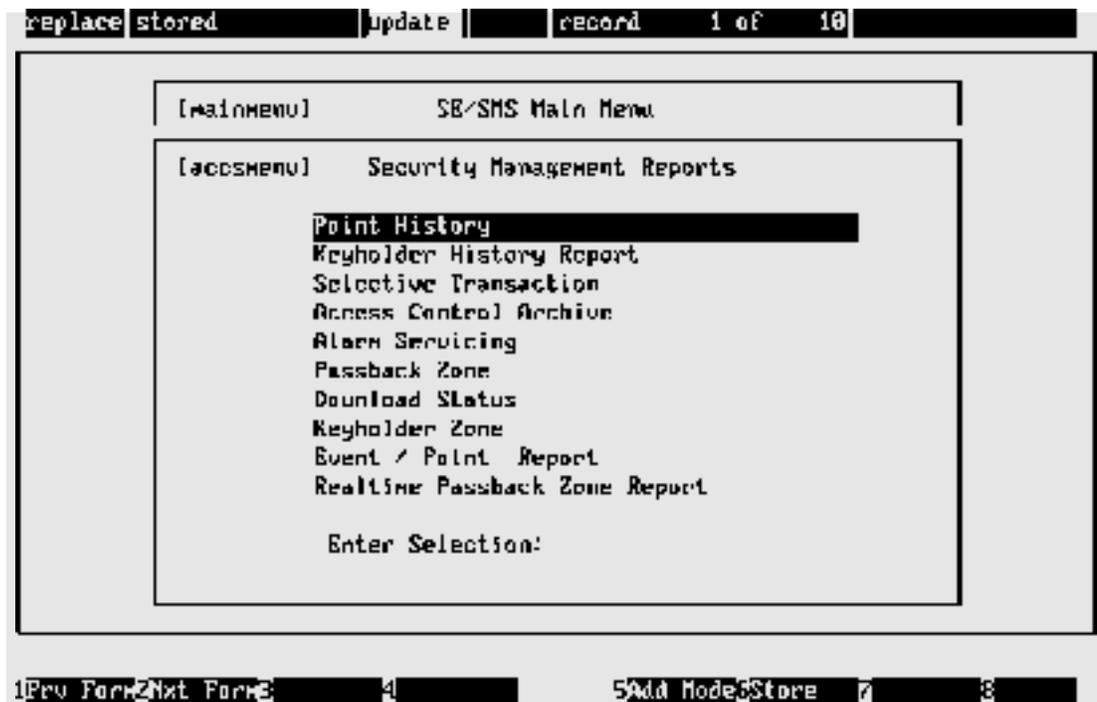
1. This feature affects the following displays and reports:
  - Monitor screen, both full- and half-screen displays
  - Review transactions screen
  - Point history report
  - Keyholder history report
  - Transaction history report - all sort options
  - Archive history report - all sort options
  
2. Log records are not altered.

# SECTION 3

# SECURITY REPORTS

## INTRODUCTION

Security management reports provide a permanent record of transactions, and are also used to examine specific events. The reports are accessed through the security management reports menu screen, [accsmenu], via the main menu. In this section, the reports are documented following the security management reports menu sequence (see section table of contents). A sample [accsmenu] screen follows:



All screens in this section show the system default values, with most screen fields requiring a numeric range entry. For example, the default range for keyholders is 1 — 999999999 (to reduce waiting time while a report is generating, enter the smallest range of numbers for each category which will still provide the information required). Other screen fields include choices for a specific data item, date ranges, regular or extended information, and report sequencing. When all fields have been entered, press Enter (Yes - default) to begin report generation:



Once compiled, a report output selection displays. Normally, 1 (system report printer) or D (display at terminal) is chosen. Report totals are printed at the end of each report.

**NOTE**

1. Some reports are over-wide (132 characters instead of the standard 80 characters), and have been formatted to use a smaller print size not available with some terminals (HP printers can handle the smaller print). These reports can be displayed but will 'wrap'; that is, some lines continue to the next display line. In such a case, use the display option to check report details, then use one of the print options to create a hard copy of the report.
2. For color PCs with Reflections 4 software, or an HP700/44, the display automatically changes to the 132-column mode for any reports with lines exceeding 80 characters.

**POINT HISTORY REPORT**

The point history report, [phstrprt], lists transaction activity at a specific point. The report lists the key number and name (if any) associated with a transaction, date and time, and description. To facilitate processing, only the last 20 transactions are used. If more than the last 20 transactions are required, use the transaction history report. A sample [phstrprt] screen follows:

```
[phstrprt]      Point History Report
Point ID: 8218 = RADIATION LAB #8218
```

**Point History — Sample Report**

| KeyhldID | Keyholder Name  | Date     | Time     | Access Description    |
|----------|-----------------|----------|----------|-----------------------|
| 166603   | HALSTON RICHARD | 06/24/96 | 16:50:47 | MANUAL LOCK           |
| 166603   | HALSTON RICHARD | 06/24/96 | 16:50:46 | MANUAL OPEN           |
| 166755   | GREENE LORRAINE | 06/24/96 | 16:50:45 | MANUAL LOCK           |
| 166755   | GREENE LORRAINE | 06/24/96 | 16:50:44 | MANUAL OPEN           |
| 161221   | ROBINS JAMES    | 06/24/96 | 16:50:43 | MANUAL LOCK           |
| 161221   | ROBINS JAMES    | 06/24/96 | 16:50:42 | MANUAL OPEN           |
| 163878   | COUSINS TERRY   | 06/24/96 | 15:09:23 | MANUAL LOCK           |
| 163878   | COUSINS TERRY   | 06/24/96 | 15:09:21 | MANUAL OPEN           |
| 165446   | AVERY JOE       | 06/21/96 | 14:19:22 | UNABLE TO UNLOCK DOOR |
| 165446   | AVERY JOE       | 06/21/96 | 13:55:47 | UNABLE TO LOCK DOOR   |

**KEYHOLDER HISTORY REPORT**

The keyholder history report, [chstrprt], lists activities for a specific keyholder. Also, the report can be used for tracking actions taken by a system operator. The report contains point or sensor data showing where activity occurred, date and time, and description. To facilitate processing, only the last 20 transactions are used. If more than the last 20 transactions are required, use the transaction history report. A sample [chstrprt] screen follows:

```

{excprprt}   Keyholder History Report

Keyholder ID   Keyholder Name   STEVEN
12345         MCCARTHY
  
```

### Keyholder History — Sample Report

| 06/27/96<br>14:36 |                      | Packlett Industries<br>Point History |          | PAGE 1         |
|-------------------|----------------------|--------------------------------------|----------|----------------|
| Point             | Point Description    | Date                                 | Time     | Access Type    |
| Keyholder         | 2771 Dale, Deborah   |                                      |          |                |
| 0225              | RDI-8082-SEN2        | 06/27/96                             | 09:32:52 | ACCESS GRANTED |
| 0221              | RDI-8082-SEN1        | 06/27/96                             | 07:34:24 | ACCESS GRANTED |
| 0215              | RDI-8081-SEN1-READER | 06/27/96                             | 07:34:22 | ACCESS GRANTED |
| 0220              | T&A READER 3 N/A     | 06/26/96                             | 15:40:42 | MANUAL OPEN    |
| 0210              | T&A READER 2 OUT     | 06/26/96                             | 15:40:40 | MANUAL OPEN    |
| 0200              | T&A READER 1 IN      | 06/26/96                             | 15:40:34 | MANUAL OPEN    |
| 0120              | ELEVATOR FREIGHT CAR | 06/26/96                             | 15:40:31 | MANUAL LOCK    |

## TRANSACTION HISTORY REPORT

The transaction history report, [excprprt], lists all transactions according to selected criteria. The transaction report function is used to create a who, what, where, and when report of all transactions. This function includes information about the ID and description of the point or sensor where the transaction occurred, the zone number of the point or sensor, the date and time of the transaction, the type of access (for an access transaction) and the ID and name of the keyholder involved with the transaction, if any. Two report types are available: short and extended. The short report accesses all standard information; the extended report does the same but includes user-defined field information. A sample [excprprt] screen follows:

| [Excerpt] Transaction Report |          |   |            |       |       |
|------------------------------|----------|---|------------|-------|-------|
|                              | Lower    | Upper                                   |            | Lower | Upper |
| Point ID                     | : 0      | 9999                                    | Dept       | : 0   | 9999  |
| Keyholder ID                 | : 0      | 999999999                               | Location   | : 0   | 9999  |
| Transaction Type             | : 0      | 999                                     | Job Cat    | : 0   | 99999 |
| Date/Time Processing:        | 0        | 0 = Range                               | 1 = Period |       |       |
| Transaction Date:            | XXXXXXXX | 11/15/95                                | Shift      | :     | zzzz  |
| Transaction Time:            | 0        | Z359                                    | Status     | :     | zzzz  |
| Zone Number                  | : -1     | 9999                                    | Tenant     | : 0   |       |
| Company                      | 0        | 9999                                    |            |       |       |
| Print Extended Info:         | M        |   |            |       |       |
| Sort Sequence                | : 1      | 1 = Point ID, Date, Time                |            |       |       |
|                              |          | 2 = Keyholder ID, Date, Time            |            |       |       |
|                              |          | 3 = Transaction Description, Date, Time |            |       |       |
|                              |          | 4 = Date, Time                          |            |       |       |

### Transaction History — Sample Report

| 11/15/96<br>10:34 |                   | SHARPSMITH LABS, INC.             |          |          |                  |           | Page 1          |        |  |
|-------------------|-------------------|-----------------------------------|----------|----------|------------------|-----------|-----------------|--------|--|
|                   |                   | Access Control Transaction Report |          |          |                  |           |                 |        |  |
| Point             | Point Description | Zone                              | Date     | Time     | Access Type      | Keyholder | Keyholder Name  | Key No |  |
| 1                 | HOST              | 801                               | 10/28/96 | 11:12:00 | FORGIVE PASSBACK | 661094    | Stanling, Bob   | 34421  |  |
| 1                 | HOST              | 0                                 | 10/28/96 | 11:23:00 | REPACK OK        |           |                 |        |  |
| 1                 | HOST              | 801                               | 10/28/96 | 13:37:00 | FORGIVE PASSBACK | 662886    | Jonesman, Linda | 32211  |  |
| 1                 | HOST              | 001                               | 10/28/96 | 14:12:00 | FORGIVE PASSBACK | 656633    | Buchmann, G.T.  | 34588  |  |
| 1                 | HOST              | 0                                 | 10/28/96 | 14:17:00 | REPACK OK        |           |                 |        |  |
| 1                 | HOST              | 0                                 | 10/28/96 | 14:49:00 | FORGIVE PASSBACK | 641918    | Saunder, Rick   | 34876  |  |

### ACCESS CONTROL ARCHIVE REPORT

The access control archive report, [acrtrprt], is identical to the transaction history report (previous report) except that it reads data from an archive tape rather than from the system database.

### ALARM SERVICING REPORT

The alarm servicing report, [almarprt], details actions taken by operators in response to alarms. A sample [almarprt] screen follows:

```

[almacprt]      Alarm Servicing Report

                Lower Limit  Upper Limit
Point ID       : 0          9999
Alarm Date     : #####     11/15/95
Alarm Time     : 0          235959
Alarm Zone     : 0          9999
Serviced By    : 0          999999999
Tenant Number: 0

Sort Sequence: 1  1) Date, Time, Point
                  2) Zone, Date, Time
                  3) Point, Date, Time
                  4) Serviced By, Date, Time

```

### Alarm Servicing — Sample Report

```

06/27/96                               PacAtlantic Racing                PAGE 1
15:01                                   Alarm Master List

Alarm No  Alrmtime  Alrmdate  Point  Zone  Resp Time  Resp Date  Clear Time  Clear Date  Serviced By
-----
Point Descrip = CHEMICALS GPS 3
  2851  09:18:00  06/26/96   20    3  14:19:05  06/26/96  11:10:10   06/26/96  Maintenance

Operator Response:                       Alarm Instructions:
CALLED FIRE DEPT.                         PUT ON MASK
CLEARED BUILDING                           CALL FIRE DEPARTMENT IMMEDIATELY
OPENED VENTS                               EVACUATE ALL PEOPLE FROM BUILDING
LEFT BUILDING                              OPEN EMERGENCY VENTS
REENTERED WHEN ALL CLEAR                   LEAVE BUILDING

```

### PASSBACK ZONE REPORT

The passback zone report, [whowhere], lists keyholders currently present in passback zones. The summary selection provides totals by zone, while the detailed report lists specific keyholders. The source for the information is the keyholder file. A sample [whowhere] screen follows:

```

[uknowhere]      Passback Zone Report

Keyholder ID      : 0      Lower Limit  Upper Limit
Tenant           : 0      999999999
Type of Passback : 3      1) Personal
                  2) Vehicular
                  3) Personal & Vehicular

Passback Zone    : 0      0) All Zones
                  1 - 9999) Specific Zone

Summary/Detail   : 1      1) Summary
                  2) Detailed

Sort Sequence    : 1      1) Keyholder ID
                  2) Name, Keyholder ID
                  3) Tenant, Name

```

### Passback Zone — Sample Report

| Keyholder | Key No | Keyholder Name   | Tenant | Pzone | Vzone |
|-----------|--------|------------------|--------|-------|-------|
| 1055699   | 83383  | MAITLING, JACK   | 0      | -1    | -1    |
| 1061128   | 84128  | LYONS, CINDY     | 0      | -1    | -1    |
| 1086201   | 83361  | DENEUVE, DENISE  | 0      | 0     | -1    |
| 1099004   | 86660  | SMITH, PAULA     | 0      | 1     | 2     |
| 1100015   | 87083  | MACKLING, JACKIE | 0      | -1    | -1    |
| 1116345   | 88883  | FLYNN, SEAN      | 0      | -1    | -1    |

### DOWNLOAD STATUS REPORT

The download status report, [downrprt], is used to create an audit-trail of system information change attempts, the devices affected, who attempted the changes, and when and if the changes were successful. A sample screen follows:

| [downrprt]                               |              | Download Status Report |               |               |  |
|--|--------------|------------------------|---------------|---------------|--|
| Record Type: 0 = All Files               |              |                        |               |               |  |
| Starting Date ***** Ending Date 11/15/95 |              |                        |               |               |  |
| 0 All Files                              | 6 Team Desc. | 12 Zones               | 18 Instructs  | 24 ABA Config |  |
| 1 Keys                                   | 7 Emp Grps   | 13 Projects            | 19 Holidays   | 25 Maps       |  |
| 2 Points                                 | 8 Events     | 14 Proj Adrs           | 20 Elevator   | 26 DKR Config |  |
| 3 Access Codes                           | 9 Tasks      | 15 Emp Prjs            | 21 Modes      |               |  |
| 4 Time Codes                             | 10 Dialers   | 16 Reports             | 22 Devices    |               |  |
| 5 N/A                                    | 11 Overrides | 17 Fail Soft           | 23 Site Codes |               |  |

### Download Status — Sample Report

| 06/27/96 |           | Nevadia Industries     |         |     |          | PAGE 1 |          |                      |       |               |         |
|----------|-----------|------------------------|---------|-----|----------|--------|----------|----------------------|-------|---------------|---------|
| 15:03    |           | Download Status Report |         |     |          |        |          |                      |       |               |         |
| Serial # | Key Value | File                   | Descrip | Typ | Date     | Time   | Maint By | Status               | Point | Point         | Descrip |
| 21729    | 76        | 2                      | Points  | Chg | 06/27/96 | 08:34  | Paul     | Received & Processed | 0     | HOST          |         |
| 21730    | 76        | 2                      | Points  | Chg | 06/27/96 | 08:34  | Paul     | Received & Processed | 60    | 1ST CNTRLLER  |         |
| 21731    | 76        | 2                      | Points  | Chg | 06/27/96 | 08:34  | Paul     | Received & Processed | 61    | CNTRL P28081  |         |
| 21723    | 21463     | 8                      | Events  | Del | 06/27/96 | 08:31  | Paul     | Received & Processed | 0     | HOST          |         |
| 21724    | 21463     | 8                      | Events  | Del | 06/27/96 | 08:31  | Paul     | Received & Processed | 52    | BAIL C1 CNTRL |         |
| 21725    | 21463     | 8                      | Events  | Del | 06/27/96 | 08:31  | Paul     | Received & Processed | 60    | 1ST CNTRLLER  |         |
| 21726    | 21463     | 8                      | Events  | Del | 06/27/96 | 08:31  | Paul     | Received & Processed | 61    | CNTRL P28081  |         |

Possible system messages for this report are:

**Unprocessed** — Information changed in the database, but has not yet been sent to the communications program module.

**Before Transmit** — Information has been sent to the communications program module, but has not yet been sent to target device.

**Transmitted** — Data has been sent from the host to the target device, but acknowledgment has not yet been received from the target device.

**Received and Processed** — Information successfully transmitted by the host and successfully received by the target device (download completed).

**ERR Transmitting Data** — Error on host side of transmission. Normally, this means that the host communications program module was unable to complete the requested download.

**ERR Receiving Data** — Information successfully transmitted by the host, but the target device was unable to receive.

## KEYHOLDER ZONE REPORT

The report lists the most recent zone information for all keyholders that meet the search criteria; however, information is not necessarily current. A sample [kyznrprt] screen follows:

```

[kyznrprt]      Keyholder Zone Report

Keyholder ID    : 0      Lower Limit  Upper Limit
Tenant         : 0
Find By        : 1      1) Zone
                  2) Area
Zone Number     : 0      0) All Zones
                  1 - 9999) Specific Zone
Area Number    : 0
Summary/Detail : 1      1) Summary
                  2) Detailed
Sort Sequence  : 1      1) Keyholder ID
                  2) Keyholder Name Keyholder ID
                  3) Zone, Keyholder Name
  
```

### Keyholder Zone — Sample Report

| 05/12/96<br>14:41 |                | Vogler Vineyards<br>Keyholder Zone Report |       |                   |          |          | Page 1 |  |
|-------------------|----------------|---|-------|-------------------|----------|----------|--------|--|
| Keyholder         | Keyholder Name | Tenant                                    | Point | Point Description | Date     | Time     | Zone   |  |
| 10556             | MAITLING JAMES | 0   | 3120  | 808SX RDR 2       | 04/02/96 | 16:48:12 | 0      |  |
| 10564             | LYONS SHELLEY  | 0   | 3120  | 808SX RDR 2       | 04/02/96 | 16:48:12 | 0      |  |
| 10569             | MCDUFF GORDON  | 0   | 3120  | 808SX RDR 2       | 04/02/96 | 16:48:12 | 0      |  |
| 10622             | DENEUVE DENISE | 0   | 3120  | 808SX RDR 2       | 04/02/96 | 16:48:12 | 0      |  |
| 10643             | SMITH PAULA    | 0   | 3120  | 808SX RDR 2       | 04/02/96 | 16:48:12 | 0      |  |
| 10701             | HERALD RICHARD | 0   | 3120  | 808SX RDR 2       | 04/02/96 | 16:48:12 | 0      |  |

## EVENT / POINT REPORT

The event / point report, [evptrprt], lists the number of events of a particular type that have occurred at a point or within a range of points. The report is limited to the current contents of the archive history file. A sample [evptrprt] screen follows:

```

[evntprpt]                Event / Point Report

Point ID      : 0          Lower      Upper
Transaction Type: 0          9999

Date/Time Processing: 0      0 - Range  1 - Period

Transaction Date: *****  11/15/95
Transaction Time: 0          235959

Zone Number   : -1        9999

Sort Sequence : 1      1 = Point ID
                  2 = Transaction Type

```

### Event / Point — Sample Report

| 03/17/96<br>09:15 |                   | Security Electronics<br>Event/Point Report |                     | Page 1      |
|-------------------|-------------------|--|---------------------|-------------|
| Point             | Point Description | Tran.                                      | Tran. Description   | Occurrences |
| 1                 | HOST              | 231  | PROJECT DEACTIVATED | 2           |
| 1                 | HOST              | 242  | DISK ALMOST FULL    | 5           |
| 2                 | DATA BASE POLLER  | 24   | POLLER STARTED      | 1           |
| 2                 | DATA BASE POLLER  | 25   | POLLER STOPPED      | 1           |
| 4                 | 808/422 POLLER    | 222  | POLLER STOPPED      | 2           |
| 4                 | 808/422 POLLER    | 224  | POLLER STARTED      | 12          |

### REALTIME PASSBACK ZONE REPORT

The realtime passback zone report, [rpsrprt], is essentially the same report as the passback zone report (described earlier in this section), with one important difference. The realtime report is created directly from shared memory instead of from the database. This feature substantially reduces the amount of time necessary to find out where keyholders are currently located. This can be very useful for monitoring hazardous areas, or when it is important to rapidly determine the number or identity of the keyholders in a particular zone.

```

[rcpasrprt] Realtime Passback Zone Report

Keyholder ID      : 0      Lower Limit  Upper Limit
                  :      0          999999999
Tenant            : 0
Type of Passback  : 3      1) Personal
                  :          2) Vehicular
                  :          3) Personal & Vehicular

Passback Zone     : 0      0) All Zones
                  :          1 - 9999) Specific Zone

Summary/Detail    : 1      1) Summary
                  :          2) Detailed

Sort Sequence     : 1      1) Keyholder ID
                  :          2) Name, Keyholder ID
                  :          3) Tenant, Name

```

## REALTIME PASSBACK DETAIL — SAMPLE REPORT

```

03/14/96          McPowell-Angus Aviation          Page 1
15:18             Realtime Passback Detail Report

```

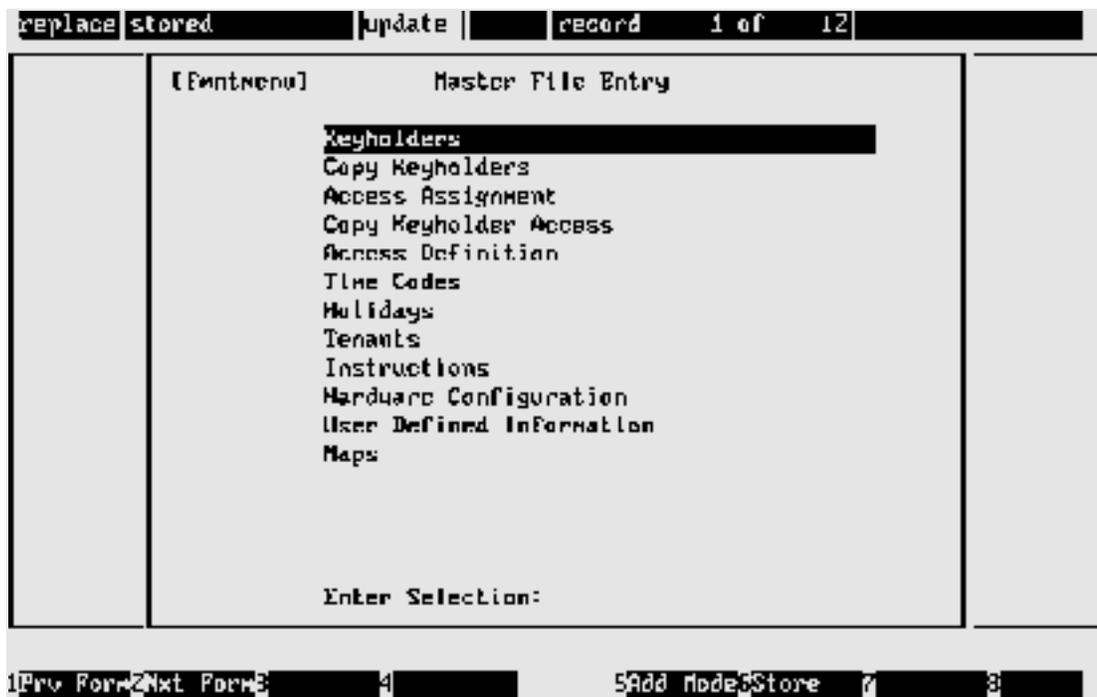
| Keyholder | Key No | Keyholder Name      | Tenant | Pzone | Vzone |
|-----------|--------|---------------------|--------|-------|-------|
| 223141    | 188954 | McDaniels, Jeff     | 0      | -1    | -1    |
| 237473    | 140226 | Wellington, Lambert | 0      | -1    | -1    |
| 233974    | 195226 | Du Pont, Michael    | 0      | -1    | -1    |
| 239965    | 200026 | Senter, Carol       | 0      | -1    | -1    |
| 248366    | 180463 | Pons, Antonia       | 0      | -1    | 7100  |
| 249037    | 143511 | Segwick, G.J.       | 0      | -1    | -1    |

# SECTION 4

# MASTER FILE ENTRY

## INTRODUCTION

The master file entry procedures are used to create and maintain the database. All initial system data is entered following the methods detailed in this section. The data item menu screens are accessed via the master file entry menu [fmntmenu], displayed via the main menu. A sample [fmntmenu] screen follows.



Some master file entry procedures are used more frequently than others. For example, keyholder data is usually added, changed, and deleted daily. On the other hand, additions or changes to system configuration information may occur only once every several months.

### Screen Access

The procedures in this section are in the order as they appear on the [fmntmenu] screen (above). Following each menu entry are the associated subscreens, again in order (the section table of contents reflects the hierarchy). After the current screen has been saved (F6), most subscreens display by pressing F2 but some display automatically.

## KEYHOLDERS

Four data entry screens are used to add new keyholders to the system, and to change or delete existing keyholder information:

1. Keyholder Entry - Page 1, [key\_entr]. Used to enter primary keyholder information.
2. Keyholder Entry - Page 2, [key1entr]. Used to enter optional keyholder information.
3. Keyholder Access Entry, [empgentr]. Used to enter access codes, access groups (keyholder access assignments), etc.
4. Project Assignment [epj\_entr]. Used to enter projects, if applicable.

The first screen, [key\_entr], is accessed from Keyholders (first item in the [fmntmenu] menu); the other screens are displayed using F2 after the previous screen has been saved.

### IMPORTANT

1. All keyholder data is linked to the keyholder ID rather than by key number or name. This allows the change or removal of key numbers from the system—a frequent requirement—without affecting entire keyholder records.
2. For future reporting purposes, we recommend that the keyholder ID record be retained when a keyholder leaves your facility. To block the keyholder ID from normal system processing, enter zero for the key number in [key\_entr], and/or delete access assignments (Esc, d, r) in [empgentr].

### Keyholder Entry—Page 1 [key\_entr]

```

[key_entr]                Keyholder Entry - Page 1
Keyholder ID: 00002779E
Last Name : LUCET          3 First Name: ELISE
Key Type: 3 Facility Code: 0000 Key Number: 1874 PIN #: 0

Tenant Number:4          = ATARAXIA ELECTRONICS, INTERNTL
Company :5              = TECHNICAL PUBLICATIONS
Dept :2                 = SOFTWARE ENGINEERING
Location :2            = SANTA CLARA, CA - TECHMART BLD
Job Cat :7             = SENIOR TECHNICAL WRITER
Shift :1               = 0000 1700
Status :1              = FT - EXEMPT
Issue Date : 10/27/94    Issue Time: 14:31
Return Date : *****  Return Time: *****
Visitor: N              Trace: N                Privileged: Y
Personal Zone : 1       = ALPHA LAB ZONE
Vehicular Zone: 1      = ALPHA LAB ZONE

PRESS <F2> (NEXT FORM) AT ANY TIME FOR PAGE 2 OR TO ASSIGN ACCESS
  
```

**Keyholder ID.** Required in the Add mode (the system denies further screen access until this field is entered). Enter a unique nine-digit maximum keyholder ID number (alphabetical letters are not supported).

**Last Name.** Optional. Enter the keyholder's last name.

**3 First Name.** Optional. Enter the keyholder's first name.

#### NOTE

Names are index-maintained rather than sequential, allowing quick keyholder record search by name or partial name.

**Key Type.** Required. Enter the key type code number:

|   |   |                       |
|---|---|-----------------------|
| * | = | No key (default)      |
| 1 | = | 1030                  |
| 2 | = | 1040                  |
| 3 | = | 1050                  |
| 4 | = | 1060 and digital keys |

Note that if the key type is unknown, use type 3. This can be changed later if necessary.

**Facility code.** Required for 1030 / 1040 key types. Enter the four-digit facility code printed on 1030 and 1040 keys; example: DO34. Default is \*\*\*\* — No facility code.

**Key Number.** Conditional. Enter an eight-digit maximum key number. If you do not wish to select a key number at this point, the system default 0 is entered automatically.

**PIN #** (personal identification number). Required if certain keypad identification equipment is used with your system (MCCI or VIP-2 poller); otherwise, disregard this field.

**Tenant Number.** Optional. Enter a four-digit maximum tenant code (*zoom* available). Default is tenant 0.

User-defined field titles. Using the control file maintenance screen (see *Control File Maintenance [ctrlentr]* in Section 6), these field titles can be changed to suit the individual user. Entries are numeric and point to a description table. (Applies also to fields *usr1* through *usr6*, and *Remarks*, in [key1entr].)

|                 |   |                                    |
|-----------------|---|------------------------------------|
| <b>Company</b>  | — | Keyholder's company name           |
| <b>Dept</b>     | — | Keyholder's department name        |
| <b>Location</b> | — | Location of keyholder's department |
| <b>Jobcat</b>   | — | Keyholder's job category           |
| <b>Shift</b>    | — | Keyholder's normal working hours   |
| <b>Emp Stat</b> | — | Keyholder's status                 |

**Issue Date.** Optional. Enter the date that the access control card for the keyholder will become valid. Default is current system date. Note that a future date will not permit access until that date is reached.

**Issue Time.** Optional. Enter the time that the access control card for the keyholder will become valid. Note that this only applies with host access. Default is current system time.

**Return Date.** Optional—Recommended if keyholder is a visitor (see *Visitor* below). Enter the final date that the keyholder's card will be valid. Default is **\*\*\*\*\*** — No expiration date.

**Return Time.** Optional—Recommended if keyholder is a visitor (see *Visitor* below). Enter the time on the final date that the keyholder's card will be valid. Default is *blank*—No expiration time. Note that this only applies with host access.

**Visitor.** Recommended. A Y/N field indicating if the keyholder is a visitor. If Y, it is advisable to enter a return date and time (previous fields). Note that this is listed for reference only. Default is N.

**Trace.** Optional. A Y/N field indicating if the keyholder is to be monitored (movements traced while in the building). Trace monitors doors, readers, and records. Using Trace causes an extra key trace log message. This feature is sometimes desirable if the keyholder is a visitor (see previous field). Default is N.

**Privileged.** Conditional. A Y / N field for ACUs supporting building modes and global anti-passback. Enter Y if this keyholder can change building modes at a remote reader and is immune from anti-passback. Default is N.

**Personal Zone.** If passback is in effect, the zone where the keyholder is currently located and reported to the system by the reader last used by the keyholder. When setting up the database, use the default (-1, unknown).

**Vehicular Zone.** The zone (car park) where the keyholder's vehicle is currently located; reported to the system by the parking lot reader last used by the keyholder. When setting up the database, use the default (-1, unknown).

## Keyholder Entry—Page 2 [key1entr]

The data entered in this screen is for information only. Field entry is self-evident (field titles *usr1* through *usr6*, and *Remarks*, can be changed to suit the individual user (see *Section 6: System Administration*). Note that data is unique and not selected as table reference (see user-defined field titles, reference 9). Simply complete those fields required by your company, store (F6), then press F2 to display the access assignment screen [empgentr].

---

```

[keyholder]          Keyholder Entry          Page 2
Keyholder Id: 27799      LUCET              ELISE
Address : 2242 SAN ANSELMO DRIVE           Phone: (484) 897-6543
          VISTA DE LOS RIOS, CA 95999      Social Security #: 123-45-6789

usr1  : HIRE DATE 12/01/91                Title: SA, TECHNICAL WRITER
usr2  : REPORTS TO M. WREISS              Floor: 2
usr3  : ████████████████████████████████ Room : 215
usr4  :
usr5  :
usr6  :
Remarks :
PRESS <F2> (NEXT FORM) AT ANY TIME TO ASSIGN ACCESS TO THIS KEYHOLDER

```

### Keyholder Access Entry [empgentr]

```

[empgentr]          Key Holder Access Entry
  ① Access          ② Access          ③ Access
Code Access Code Description SFS Group Access Group Description Override
2 █████ DUNLD SACS ALPHA LAB 888SX N B

```

**Access Code.** Optional. Enter an access code number that applies to this keyholder (the system automatically enters the access code description). Default is 0—No access code.

#### NOTE

There is no limit to the number of access codes that can be assigned, with the following two exceptions:

1. Do not assign a keyholder more than one access code for a single NexSentry, 8xx series, or 422 ACU.
2. The system will not allow you to combine two access codes with the same download device ID number in one access group.
3. Do not assign two access groups with codes for the same download device ID.

**SFS** (smart failsoft option). Optional. Smart failsoft access codes are used when communications between the host and ACU are disrupted for more than 15 seconds. Enter

Y if the downloaded access code is to be sent to the ACU as a smart failsoft access code. Default is N. Note that this is used only in conjunction with the host access codes.

**NOTE**

The smart failsoft option is not supported with any keys used in conjunction with 708P and 718P ACUs, but a function is built in to the units which does provide some measure of failsoft protection in the event of a communications failure with the host.

The 708P and 718P ACUs can be programmed to accept up to 25 command keys, and access is allowed when these are presented (eight doors maximum). Usually, the command keys selected are those issued to managerial and engineering staff, and to persons responsible for building maintenance.

This feature is limited to some extent in that time codes cannot be used in conjunction with this special programming, and event entries (door opening records, in this case) are not logged.

- ③ **Access Group.** Optional. Enter an access group number (no limit) that applies to this keyholder (the system automatically enters the access group description). Default is 0—No access group.

**Note**

There is no limit to the number of access codes that can be assigned, with the following two exceptions:

1. Do not assign a keyholder more than one access code for a single NexSentry, 8xx series, or 422 series ACU.
2. The system will not allow you to combine two access codes with the same download device ID number in one access group.
3. Do not assign two access groups with codes for the same download devices.

- ④ **Access Override.** Optional (*zoom* available). Enter the access override code that applies to this keyholder. Default is 0—No access override code.

**Project Assignment [epj\_entr]**

If the keyholder has been assigned to a project, enter the project number using the [epj\_entr] screen (multiple projects can be assigned). Display this screen by pressing F2 after the access assignment screen (previous screen) has been saved (F6). Note that the project function will not work properly unless the host provides access control.

A sample [epj\_entr] screen follows. Enter the project number (*zoom* available) then press Enter; the project description displays automatically. If multiple projects are to be assigned, enter and store each one separately.

```

[epj_entr]      Project Assignment

Project  Project Description
  5      EMERGENCY CIRCUIT BOARD REVISION PROJECT
  
```

## COPY KEYHOLDERS

### Copy Keyholder Information

Used when creating new keyholders who share data with existing keyholders, the [key\_copy] screen is an important timesaving feature. A sample screen follows:

```

[key_copy]      Copy Keyholder Information

      Keyhld ID  Key Num  Last Name  First Name
1 (From) 27786   1867    MILLAR    JOHN
2 (To)  27793   1874    GREV      JANE
  
```

**From.** Enter an existing keyholder ID (*zoom* available). The system automatically supplies the key number and the keyholder names.

**To.** Enter the new keyholder ID, new key number and new keyholder name.

System responds with Okay to continue? When complete. Enter Y and a new keyholder record for the To keyholder is automatically created, with identical parameters as the From keyholder. Changes and corrections for the new ID are made as required using the various keyholder data entry screens.

## ACCESS ASSIGNMENT

### Keyholder Access Assignment [egrpentr]

The [egrpentr] and [egrpentr1] screens, accessed from *Access Assignment* (third item in the [fmntmenu] menu), are used as a fast way to make access assignments without using the keyholder data entry screens. Data entry is the same as for the keyholder access entry screen [empgentr]. The keyholder access allows only assignment permissions without access to keyholder screen. A sample screen showing [egrpentr] and [egrpentr1] follows:

| [egrpentr1] |             | Keyholder Access Assignment Entry |           |              |              |             |                 |
|-------------|-------------|-----------------------------------|-----------|--------------|--------------|-------------|-----------------|
| Access Code | Access Code | Description                       | SFS only? | Access Group | Access Group | Description | Access Override |
| 2           | DWMLD 003   | ALPHA LAB B00SX                   | M         | 0            |              |             | 0               |

### COPY KEYHOLDER ACCESS [ergcopy]

The copy keyholder access screen, [ergcopy], is used in the same way as the copy keyholder information screen for copying keyholders with similar access assignments. This is especially useful where multiple codes/groups are assigned on keys.

| [ergcopy]    |        | Copy Keyholder Access |         |       |
|--------------|--------|-----------------------|---------|-------|
| Keyholder ID | <From> | 27793                 | LUCET   | ELISE |
| Keyholder ID | <To>   | 20003                 | RALSTON | JERRY |

---

## ACCESS DEFINITION

---

The access definition selection in the master file entry menu displays the access definition menu:

- Access Code Entry, Access Code Definition, Elevator Definition
- Access Group Entry, Access Group Definition
- Access Override Entry
- Fail Soft Entry
- Project Definition

### ACCESS CODE ENTRY [acdsentr]

Access codes are created using the access code entry [acdsentr] and the access code definition [acodentr] screens. A third screen, [eleventr], is used for elevator codes.

Three access code types are identified—Centralized (Host); Distributed; Smart Failsoft:

**Centralized (Host)**—Used when the host computer makes access decisions. An example is with global anti-passback, where in/out readers may be connected to different ACUs.

**Distributed Access Codes** — Distributed access codes are created for each ACU and are downloaded from the host. When a card is presented to a reader, the ACU makes the access decision. In some circumstances, the host computer may override an access request denied by an ACU.

**Smart Failsoft** — These codes work only if the ACU is in smart failsoft mode. This occurs when communication between the host and the ACU is interrupted for more than 15 seconds. During normal operation (ACU communicating with the host), access requests from keyholders with smart failsoft status are passed to the host for decision.

#### NOTE

Smart failsoft is not supported with 1050 keys used in conjunction with 708P and 718P ACUs, but a function is built in to the units which does provide some measure of failsoft protection in the event of a communications failure with the host. The ACUs can be programmed to accept up to 25 specific command keys, and access is allowed when these are presented (access may be for one to eight doors). The feature is limited to some extent in that time codes cannot be used in conjunction with this special programming, and event entries (door opening records, in this case) are not logged.

A sample [acdsentr] screen follows:

---

```

[acdsentr]      Access Code Entry
1 Access Code ID: 15
2 Tenant       : 0 - ALL ENCOMPASSING
3 Download Device ID: 001
4 Code Description : SBAESX ELEVATOR CODE
PRESS <F2> TO ASSIGN READERS & TIMES TO THIS ACCESS CODE

```

**Access Code ID.** Required. Enter a four-digit maximum access code number.

**Tenant.** Required (*zoom* available). Enter a four-digit maximum tenant code number. Default is tenant 0.

**3 Download Device ID.** Optional (*zoom* available). This field must be used if the access code being created is to be downloaded to an ACU—enter the ACU ID number. Enter **0** (default) if access decisions for this code are to be made by the host.

**4 Code Description.** Required. Enter a 30-character maximum description of the access code, e.g., REGULAR DAY SHIFT, WEEKEND RECEIVING.

When screen entry is completed press F6 to store the data; the access code definition screen, [acodentr], displays automatically.

### ACCESS CODE DEFINITION [acodentr]

This screen is used to enter the reader ID and time codes (four maximum per reader) that will apply to this access code. Each reader ID entered must be added (F5) and stored (F6) individually. When you finish data entry for this screen, press F6 again to store the completed access code definition. A sample screen follows:

```

[acodentr]      Access Code Definition
1 Reader ID      2 Time Code
   Description   Code  Range  Mon Tue Wed Thu Fri Sat Sun Hol
0123 TIM'S SBAESX DOOR 2 1 00:00-23:59 Y Y Y Y Y Y Y Y
0 00:00-00:00 N N N N N N N N
0 00:00-00:00 N N N N N N N N
0 00:00-00:00 N N N N N N N N
FOR ELEVATOR CONTROL READERS. PRESS <F2> <Nxt Form> TO ASSIGN OUTPUTS

```

If this access code is to be assigned to an elevator reader, press F2 after entering the Reader ID and Time Code fields. See *Elevator Access Codes*—following subsection.

Note that this action may only be done for readers defined as elevator reader types in the reader definition screen.

**Reader ID.** Required. Enter the reader number to be linked to this access code (the reader description is automatically displayed). The reader numbers can be entered in any order.

**Time Code.** Optional. Enter up to four time codes, in any order, that apply to this access code (the time code parameters are displayed automatically). Default is 0 which is no access.

### ELEVATOR DEFINITION [eleventr]

The elevator definition screen must be completed if the reader type is an elevator reader (reader type 5). Perform the following steps:

1. When the Reader ID and Time Code fields have been entered in [acodentr], press F2 to display the elevator definition screen [eleventr]—example below.
2. Enter the output contact IDs (usually wired to the elevator cab floor buttons) to be closed (activated) when access is granted via this reader. Store each item (F6) after entry. Use F5 to move to the next output contact ID line.

```
[eleventr] Elevator Definition
Reader/Point Id
      8004 = Contact 4
      8006 = Contact 6
      8008 = Contact 8
```

### ACCESS GROUP ENTRY [agdsentr], [agrpentr]

To facilitate assigning similar access privileges to large numbers of keyholders, the system allows two or more access codes to be combined into an access group. Two screens are used: [agdsentr] and [agrpentr]. Sample screens follow.

```

1 [agdsentr]      Access Group Entry
2 Access Group ID : 12
3 Tenant          : 2 = BETA COMPUTERS
Group Description: WEEKEND UNSKED TESTING
```

**Access Group ID.** Required. Enter a four-digit maximum access group number.

**Tenant.** Required (*zoom* available). Enter a four-digit maximum tenant number. Default is tenant 0.

- ③ **Group Description.** Required. Enter a 30-character maximum description of the access group.

When screen entry is completed press F6 to store the data, at which point the *Access Group Definition* screen displays automatically. This screen permits you to enter the access codes that will apply to this access group. Each access code entered must be added (F5) and stored (F6) individually. When you finish data entry for this screen, press F6 again to store the now fully completed access group.

#### NOTE

Host-controlled and downloaded access codes may be combined in the same access group, but see *Warning* at the end of this subsection.

### ACCESS GROUP DEFINITION [agrpentr]

| [agrpentr] Access Group Definition |                                | ③     |
|------------------------------------|--------------------------------|-------|
| ①                                  | ②                              | SFS   |
| Access Code                        | Access Code Description        | only? |
| 34                                 | RDI ACCESS CODE                | N     |
| 40                                 | NO OPERATION HOST ACCESS CODE  | N     |
| 57                                 | ELEVATOR ACCESS CODE           | N     |
| 88                                 | 888 ALL ACCESS DOWNLOAD        | N     |
| 88                                 | ALPHA 888SX 5100 ALLTIME/DOORS | N     |

**Access Code.** Required (*zoom* available). Enter an access code, in any order, to be linked to this access group. Each code must be added (F5) and stored (F6) individually.

**Access Code Description.** Automatically inserted by the system.

- ③ **SFS only?** (smart failsoft option). Optional. Smart failsoft access codes are used only when communications between the host and ACU are disrupted for more than 15 seconds. Enter Y if the downloaded access code is to be sent to the ACU as a smart failsoft access code. Note that this is used only in conjunction with host access codes. The default is N.

**WARNING**

1. Access codes that include the same reader(s) should not be included in the same group unless one code is a downloaded code, and it has been set up with the SFS (smart failsoft) flag set to Y. Mixing codes that include common readers with different time codes may cause unpredictable results.
2. Do not combine two access codes with the same download device ID in one access group.
3. Keyholders may have only one downloaded access code per ACU.

**ACCESS OVERRIDE ENTRY**

Access override codes are typically used for visitors to restrict or allow access to specific locations for specific time periods. This is a host function that must be used only if normal access is through host access codes:

|   | [acoventr]     | Access Override Entry  |
|---|----------------|------------------------|
| 1 | Override Code: | 2                      |
| 2 | Description:   | TOXIC CHEMICALS IN USE |
| 3 | Start Date:    | 06/06/96               |
| 4 | End Date:      | 06/10/96               |
| 5 | Permission:    | A                      |

**Override Code.** Required. Enter an override code number in the range 1—9999.

**Description.** Optional. Enter a 30-character maximum description of the override.

3 **Start Date.** Required. Enter the override start date.

4 **End Date.** Required. Enter the override end date.

5 **Permission.** Optional. Permission status. Enter A to allow access; enter D to deny access. Default is A.

## FAILSOFT ENTRY

708P ACUs can be programmed to recognize up to 25 keyholders (based on key numbers) for use when communication with the host computer is temporarily unavailable. Known as failsoft, the feature becomes active (access is granted) for these keyholders after 15 seconds following the occurrence of the communications interruption (response is not available for specific time periods, however). A sample screen follows:

| [fs_entr] |              | Fail Soft Entry           |         |
|-----------|--------------|---------------------------|---------|
| 1         | Device ID    | 7188 - 708P PARKING CNTLR |         |
| 2         | Keyholder ID | 661896 GUARD              | NEW 3   |
|           | Reader ID    | Reader Description        | Allowed |
|           | 7118         | 708 #1 ENTER ZONE A       | Y       |
|           | 7128         | 708 #2 ENTER ZONE B       | Y       |
|           | 7138         | 708#1 ENTER ZONE B        | Y       |
|           | 7148         | 708 DOOR 4                | Y       |

**Device ID.** Required (*zoom* available). Enter the device ID for which failsoft is to be assigned (the readers associated with the 708P automatically display).

**Keyholder ID.** Required (*zoom* available). Enter the applicable keyholder ID (keyholder name automatically displays).

**3 Allowed.** Optional. Enter Y or N as appropriate for the individual keyholder. Default is N.

## PROJECT ENTRY [prj\_entr], [prd\_entr]

This is designed primarily for high security facilities. Project is used to grant temporary access to selected keyholders at project-controlled doors when a project is activated, while access for all other keyholders who normally enter through these doors is temporarily denied. The projects are continually monitored by the system and are updated as project status changes from activated to deactivated, and vice versa. This is a host function that must be used only if normal access is through host access codes. A sample [prj\_entr] screen follows:

| [prj_entr] Project Entry |  |
|--------------------------|--|
| 1                        | Project ID: 52                               |
| 2                        | Description: SECURITY INSPECTION             |
| 3                        | Starting Date: 07/01/96 Starting Time: 08:00 |
| 4                        | Ending Date: 07/01/96 Ending Time: 17:30     |

**Project ID.** Required. Enter a four-character maximum project ID code.

**Description.** Optional. Enter a 40-character maximum description of the project.

- 3 **Starting Date and Time.** Enter the project's starting date and time in the formats MM/DD/YY and HH:MM.
- 4 **Ending Date and Time.** Enter the project's ending date and time in the formats MM/DD/YY and HH:MM.

Store (F6) data when completed; the project definition [prd\_entr] screen automatically displays. Enter the applicable reader IDs for this project (*zoom* available). Store (F6) each ID separately when entered, then immediately press F5 to move the cursor to the next data entry point on the screen. Repeat for as many readers as are to be included in the project. A sample [prd\_entr] screen follows:

| [prd_entr] Project Definition |                      |
|-------------------------------|----------------------|
| Header Id                     | Header Description   |
| 1001                          | 422 ENTRY #1         |
| <b>1B1C</b>                   | 818 #7 DOOR #1 ALPHA |

## TIME CODES [tmcdentr]

Time codes are normally used to define when points and readers are active. The codes are also used to automatically lock / unlock doors, activate / deactivate output relays, and to initiate recurring tasks. When combined with readers into access codes, the time codes define when access is valid for particular readers. A sample [tmcdentr] screen follows:

```

[tmcdentr]           Time Code Entry
  1 Time Code #: 20  2 - SPECIAL MODIFIED TIME CODE
  3 Start  4 End  5 Mon Tue Wed Thu Fri Sat Sun Hol
    07:00 16:59  Y  Y  Y  Y  Y  N  M  N
  
```

**Time Code #.** Required. Enter a two-digit (maximum) time code. If the time code is omitted, the system defaults to time code 0 (zero). The default time code description is NEVER ACTIVE, with start/end times of 00:00 and N (no) for all the day entries.

= (description). Optional. Enter a 30-character maximum description of the time code.

- 3 **Start.** Required. Enter a start time using 24-hour notation with an intervening colon. Examples: 08:45 (8:45 a.m.), 19:15 (7:15 p.m.). If the start time is entered incorrectly, the system either prevents further data entry or displays an error message (press Enter to return to data entry). In both cases, reenter the time code using the correct format.
- 4 **End.** Required. Enter an end time. All details for the Start field pertain.
- 5 **Mon through Hol.** Optional. The field represents the days of the week and holidays. Enter Y or N as applicable for the new time code. Default is N.

## HOLIDAYS [hol\_entr]

Annual holidays must be entered into the system. The information is required so that the host computer can determine whether access codes, auto-unlock functions, etc., need to be handled differently for the specified holidays.

```

[hol_entr]           Holiday Entry
  1 Holiday Date: 11/28/96
  2 Holiday Name:  THANKSGIVING
  
```

**Holiday Date.** Required. Enter a date in the format MM/DD/YY (the system supplies leading zeroes where applicable).

**Holiday Name.** Optional. Enter a 20-character maximum holiday name.

## TENANTS [tententr]

Two or more companies or groups can operate a single SE 6000 system, and they are referred to as tenants. (If required, the system can also be configured to allow individual tenants to share components.) Tenants may be unrelated occupants of the same or different facilities who use a single SE 6000 to view and manipulate only that data which applies to them. One of the tenants in a multiple tenant usage is the system owner who controls and has access to the entire system at all times. The systems owner may also be the system administrator. The default tenant code is 0 (zero), usually the system owner, who has access to the entire system at all times. A sample [tententr] screen follows.

```

1  [tententr]          Tenant Entry
2  Tenant Number:    [ ]
   Tenant Name :    WESTINGHOUSE SECURITY ELEC.

```

**Tenant Number.** Optional. Enter a 4-digit maximum tenant number. Default is tenant 0.

**Tenant Name.** Optional. Enter a 30-character maximum tenant name.

## INSTRUCTIONS [instentr]

Specific instructions are entered into the system to direct operators as to the action to be taken when a specific point is activated (usually in response to an activated alarm). The instructions display automatically on the alarm response screen, or may be selectively viewed from the realtime control maps. A sample [instentr] screen follows:

```

1  [instentr]          [Instruction Entry]
2  Point ID   : 5100 - ALPHA LAB HBRSX 1
3  Tenant    : 7     ALPHA LAB TELHS

Instructions: CALL FIRE DEPARTMENT 123-4567
              ACTIVATE LAD EVACUATION STERN
              DIRECT FIRE DEPARTMENT CREW TO SCENE
              UPDATE EVENT LOG
              NOTIFY BUILDING OPERATIONS MANAGER
              BEEPER= 54321 (988) 987-6543
              *****
              *****

```

**Point ID.** Required (*zoom* available). Enter the point ID to which this instruction applies.

**Tenant.** The tenant number entered when this point was created is automatically entered into this field.

- 3 Instructions.** Eight 40-character lines are provided for detailed instruction entry. Refer to the sample screen for an example.

## HARDWARE CONFIGURATION [confmenu]

The hardware configuration item in the master file entry menu displays the hardware configuration menu [confmenu]:

- Zones
- Areas
- Pollers
- Devices
- Readers
- Points
- Auto Opens/Activates
- Device Report Definition
- SE 422 PIN Definition
- SE 422 Hardware Definition
- Dialer Entry
- Site Entry Definition
- ABA Configuration Entry
- DKR Configuration Entry

## ZONES [ZONEENTR]

Zones comprise user-selected system components grouped to facilitate system operation and administration, and are required if the anti-passback feature is to be used. Zones may be defined for vehicles as well as keyholders. A sample [zoneentr] screen follows:

```

[zoneentr]           Zone Entry
1 Zone Number:      1
2 Zone Name :      ALPHA LAB ZONE
3 Passback Area :  N
4 Passback Type :
5 Passback Level:
  
```

**Zone Number.** Required. Enter an four-digit maximum zone number. There is no default for this field.

**Zone Name.** Optional. Enter a 30-character maximum tenant name. If this field is omitted, the system fills the field with asterisks.

- 3 **Passback Area.** Optional. This field is used to indicate if passback is in effect for this zone. Enter P if personnel passback is used, V if vehicle passback is used, N if passback is not used. The default is N.
- 4 **Passback Type.** Required if passback (field #3) is either P (personnel) or V (vehicle) for this zone. Enter H for hard passback; S for soft passback. Hard passback prevents access if already in the zone; soft passback allows access and generates a passback violation message. There is no default for this field.
- 5 **Passback Level.** Required if passback (field #3) is either P (personnel) or V (vehicle) for this zone. Enter G for global (host-controlled); L for local (ACU-controlled). There is no default for this field.

## AREAS [areaentr], [areaentr1]

For reporting purposes only, passback zones may be grouped into areas. Reporting (keyholder zone report) may be by zone or area, with the area report listing the zones contained in each area. Assign a number and optional description for the area using [areaentr]; enter the applicable zone numbers in [areaentr1]. Note that for local passback zones, ensure that both in and out readers are controlled by the same ACU. A sample screen showing [areaentr] and [areaentr1] follows:

```
[areaentr1]

Zone  Zone Description
1     ALPHA LAB ZONE
2     HARD PASSBACK TEST ZONE 2
8B1   TEST ANNUNCIATOR ZONE
81B   818 ALPHA LAB ZONE
```

## POLLERS [pol\_entr]

### IMPORTANT

The pollers and poller parameter files discussed below are normally installed and tested at the factory or by your dealer. Please consult your dealer or WSE customer support before adding, changing, or deleting poller information.

Pollers are device-specific application programs that communicate with the ACUs and the input / output controllers, and in addition to providing these communication links they perform many other tasks. For example, the pollers make access decisions, report devices that are not responding, and provide the means to reload devices with system and key data as necessary.

The SE 6000 can run different pollers or multiple copies of the same poller concurrently but, with the exception of the NexSentry, 8xx-series, and 422 ACUs, the pollers can be run with one device type only. Poller parameter files are read when the poller programs start. The parameters define the poller type, the physical port assignment, and other required control information.

Twenty-two poller types are currently in operation (codes 5, 20, 21, and 23 are not used):

|    |                    |   |  |
|----|--------------------|---|--|
| 1  | 708P               | — | 708P ACU   |
| 2  | Opto               | — | Optomux 22 alarm monitor                                   |
| 3  | Etp - Rdu          | — | Stellar RDU 2000 monitor                                   |
| 4  | Timer Poller       | — | Interactive extended processing poller                     |
| 6  | 808                | — | 8xx series / SE 422 ACUs                                   |
| 7  | MCCI               | — | MCCI keypad  |
| 8  | Parking            | — | Parking controller—Internal: No physical connection        |
| 9  | Remote Dialer Schd | — | Remote dial-up interface controller                        |
| 10 | Elevator           | — | Elevator control poller—Internal: No physical connection   |
| 11 | Database           | — | Database poller—Internal: No physical connection           |
| 12 | Burle              | — | Burle closed-circuit television (CCTV)                     |
| 13 | Vicon              | — | Vicon camera switcher                                      |
| 14 | Hand Geometry      | — | Supports up to 32 hand geometry readers                    |
| 15 | Amdi               | — | Amdi 102 / 103 magnetic stripe readers (supports up to 16) |
| 16 | Radionics          | — | 6000/6500 Receiver   |
| 17 | Nesting            | — | Nested parking timer                                       |
| 18 | Polaroid Server    | — | Not used for Polaroid ID 4000                              |
| 19 | WSE XV Poller      | — | Used for capturing images on an X-Terminal                 |
| 22 | WSE VIP2 Poller    | — | Used with numeric keypad for entry of PINs                 |
| 24 | American Dynamcis  | — | Closed circuit television (CCTV)                           |
| 25 | Pacom CCTV         | — | Closed circuit television (CCTV)                           |
| 26 | Intercom System    | — | Used to automatically switch cameras                       |

A sample [pol\_entr] screen follows:

```

[pol_entr]                               Poller Entry
1 Poller ID : 88                        2 Poller Description: 8888 POLLER
3 Tenant      : 0 - ALL ENCOMPASSING
4 Computer ID: 0                        5 Poller Number: 2
6 Poller Type: 6 = 888
7 Disable: N Zone Number: 0 - N/A
8

```

**Poller ID.** Required. Enter a four-digit maximum poller number. There is no default for this field.

**Poller Description.** Optional. Enter a 20-character maximum description of the poller. If omitted, the poller ID number is inserted by default.

- 3 **Tenant.** Optional (*zoom* available). Enter a four-digit maximum tenant code number. Default is 0.
- 4 **Computer ID.** Required. Enter the ID of the computer on which this poller is to run. Default is 0—host computer.
- 5 **Poller Number.** Required. Enter the number of the corresponding poller-parameter file. Refer to the configuration sheet detailing the factory-assigned poller numbers.
- 6 **Poller Type.** Required. Use the zoom feature (F7) to access the Poller Type Display screen. Once there, arrow down to the required poller type, press F1, and the poller type number is entered automatically into the *Poller Entry* screen.
- 7 **Disable.** Not currently implemented.
- 8 **Zone Number.** Required. Enter a four-digit maximum zone number. Default is 0.

## DEVICES

The most common devices used with SE 6000 system are the WSE NexSentry, 708P, 8xx-series and 422 ACUs. Other devices supported include:

- Opto 22 input / output controllers
- CCTV switchers
- Radionics alarm panels
- One or more additional SE 6000 systems used as local controllers

With the exception of the NexSentry, 8xx-series and 422 ACUs, each individual device type requires its own poller and associated hardware port assignment.

## SIMPLE / INTELLIGENT DEVICE TYPES

The terms *simple* and *intelligent* are often used to describe certain device types used in conjunction with the SE 6000.

**Simple Devices.** With simple devices, the SE 6000 makes the access decisions and also instructs the device to take various actions. The 708P ACU is a simple device, for example.

**Intelligent Devices.** Depending on system configuration requirements, intelligent devices can be programmed to make their own decisions concerning access and actions to be taken. The devices typically have their own application software and / or firmware, and they maintain their own internal data files which are used for decision making. The NexSentry, 8xx-series, and 422 ACUs are intelligent devices, for example. As required, the intelligent devices can be set up to be

controlled exclusively by the SE 6000 (*deferred mode*), to operate entirely independently of the SE 6000 (*local mode*), or a combination of both.

## DEVICE ENTRY SCREENS

The following screens are used when setting up device types:

- 8xx-series ACUs — [dev\_entr], [d808entr]
- NexSentry — [dev\_entr], [nexsentr], [d818entr]
- 818-series ACUs — [dev\_entr], [d808entr], [d818entr]
- 422 ACUs — [dev\_entr], [d422entr]
- All other devices — [dev\_entr]

## DEVICE ENTRY [dev\_entr] — ALL DEVICE TYPES

Complete the [dev\_entr] screen when setting up any device. A sample screen follows:

```

[dev_entr]                Device Entry
  1 Device ID: 181E        2 Device Description: RDI 808SX S MODE =1
  3 Tenant : 0 - ALL ENCOMPASSING
  4 Computer ID: 10      5 Poller Number: 1        6 Address: 1
  7 Device Type:         4 = 808S
  8 Watch Dog Timer Count: 0
  9 Disable: M         10 Zone Number: 988 = RDI ZONE
PRESS <F2> TO DEFINE DEVICE CONFIGURATIONS FOR 808'S ONLY
  
```

**Device ID.** Required. Enter a unique, four-digit maximum device ID number in the range 1—9999.

**Device Description.** Optional. Enter a 20-character maximum description of the device. If omitted, the system enters the device ID number in this field.

- 3 **Tenant.** Optional (*zoom* available). Enter the tenant number applicable for this device. Default is 0.
- 4 **Computer ID.** Required. Enter the ID of the computer that connects to this poller. Default is 0 (host).
- 5 **Poller Number.** Required. Enter the number of the poller that connects to this device. This information is available from your system installer and should be obtained before beginning screen entry.

- 6 Address.** Required. Enter the address of the device. Since each poller can poll a number of devices, the *Address* field is necessary to tell the host which device to poll. The address ranges are included in the *Device Type* table (see following field). Note that the system will not allow duplicate device addresses on the same poller.
- 7 Device Type.** Required (*zoom* available). Enter the device type number in the range 1 through 23 (field 20 and 22 are not currently used):

| Type | Description      | Address Range (see previous field) |
|------|------------------|------------------------------------|
| 1    | Host             | 1 only                             |
| 2    | Controller       | 1 — 8                              |
| 3    | 708P             | 1 — 8                              |
| 4    | 808S             | 1 — *16                            |
| 5    | Opto             | 0 — 15                             |
| 6    | Etp              | 1 — 16                             |
| 7    | MCCI             | 1 — 16                             |
| 8    | RDI              | 1 — 32                             |
| 9    | RLC              | 1 — 8                              |
| 10   | 808SX/SN         | 1 — *16                            |
| 11   | 818SX/SN         | 1 — *16                            |
| 12   | AMDI 102/103     | 1 — 16                             |
| 13   | NexSentry        | 1 — 16                             |
| 14   | Camera           | 1 only                             |
| 15   | SE422            | 1 — *16                            |
| 16   | Radionics        | 1 only                             |
| 17   | Polaroid ID 4000 | 1 — *16                            |
| 18   | 818SC            | 1 — *16                            |
| 19   | 808SXT           | 1 — 16                             |
| 21   | WSE VIP2         | 1 — 16                             |
| 23   | Timer Device     | 1 only                             |

\*Note that these are limited to 8 if used with host access.

- 8 Watch Dog Timer Count.** Required for Opto 22 devices only. Indicates the action to be taken if communication is interrupted between the host computer and the device. Enter:
- 0 — No action (default)  
 1 — Open on time-out  
 2 — Close on time-out
- 9 Disable.** Required. A Y/N field indicating if the device is to be shunted at system start up (Y). This is recommended to disable devices until they are physically connected into the system. Default is N (device not shunted).
- 10 Zone Number.** Required (*zoom* available). Enter the zone number applicable for this device. Default is 0.

## SE 8XX-SERIES DEVICE CONFIGURATION ENTRY [d808entr]

The [d808entr] screen must be completed for all 8xx-series ACUs (use F2 to display the screen after the previous screen has been stored). A sample screen follows:

```

1  [d808entr]          808 Device Configuration Entry
   Level] Name       Password
1>  1  OPER1        PASS1
2>  A  OPER2        PASS2
3>  B  TESTB        NEWB
4>  C  TESTC        NEWC
5>  D  TESTD        NEWD
6>  E  TESTE        NEWE
7>  F  TESTF        NEWF
8>  F  TESTG        NEWG

10 808 Modem Definition:
*****
*****
*****

11 Number Of Retry Times: ***
12 KON/XOFF: Terminal Port N Host Port N
14 Building Closed Timescodes: Tmc01: 0 Tmc02: 0 Tmc03: 0 Tmc04: 0
13 Building Open Reminder: 0

2  Report Definition
3  Tamper      : 1
4  Power Fail: 1
5  Override   : 1
6  Key Definition
7  Type       : 0 = NONE
8  Aux. Type  : + =
9  Facility   : ***
7  Alt Facility: A000
8  Auto Forgive
9  Time Code 1: 0
9  Time Code 2: 0
9  Time Code 3: 0
9  Time Code 4: 0

```

**Level, Name, Password.** Required. These first three fields are entered to identify up to eight operators who will be permitted to set/change system parameters for a particular ACU from the ACU terminal port. User 1 must be established (defaults to operator 1); operators 2 through 7 are optional. Enter the operator's security code (A through F), name and password.

The security codes A through F control the degree to which the operator may add/change/delete the system parameters from the ACU terminal port. Code A has the most privileges, code F has the least. For detailed information concerning operator privilege levels, refer to the applicable ACU manual.

### NOTE

The *Level*, *Name* and *Password* fields are specific to individual 804/808 ACUs and apply only to operators logging in directly via the ACU's terminal port. The fields are not part of the SE 6000 control parameters.

**Tamper.** Optional. Enter the tamper report number if a report has been created (see applicable ACU manual). The report states the system actions that will be taken if the ACU enclosure housing is opened. Default is 0.

- 
- 3 **Power Fail.** Optional. Enter the power fail report number if a report has been created (see applicable ACU manual). The report states the actions that will be taken by the ACU should a power failure occur. Default is 0.
  - 4 **Override.** Optional. Enter the operator override report number if a report has been created (see applicable ACU manual). The report states the actions that will be taken by the ACU if, for example, a manual unlock or a shunt occurs. Default is 0.
  - 5 **Type.** Optional. Enter the number for the key type used. Default is 0.

**NOTE**

The valid key types are as follows:

- 0 — None
- 1 — 1030
- 2 — 1040
- 3 — 1050
- 4 — 1060
- 5 — 1050 / 1060 / Digital Keys

- 6 **Aux. Type.** Conditional. Auxiliary key type. A second key type, other than the one entered in the previous field, can be entered here if applicable. Default is 0.

- 0 — None
- 1 — 1030
- 2 — 1040

Note: the previous two fields are applicable only to devices that support multiple key types.

- 7 **Facility.** Required for key types 1 and 2 (previous field). Enter the facility code assigned to the keys. Defaults to \*\*\*\* if omitted.
  - 8 **Alt Facility.** Conditional. Enter a second facility code to allow a different set of keys to be used with this ACU. Defaults to \*\*\*\* if omitted.
  - 9 **Auto Forgive.** Optional. Up to four time codes can be entered that execute the forgive command at the ACU. Default is 0 (feature disabled if all auto-forgive time codes are 0).
  - 10 **808 Modem Definition.** Not used.
  - Number of Retry Times.** Not used.
  - 12 **XON/XOFF.** Not used.
-

- 13 **Building Closed Time Codes.** Optional. Provides up to four time intervals during which the building should be closed. Default is 0.
- 14 **Building Open Reminder.** Optional. If the building should be closed (indicated by the time codes entered in the previous field), a reminder message is logged and repeated for the number of minutes specified (0 to 240). Default is 0.

## SE NEXSENTRY DEVICE CONFIGURATION ENTRY [nexsentr]

Complete the [nexsentr] screen for the NexSentry ACU and then press F2 Next Form to display the [d818entr] screen. Enter all appropriate information and press F6 Store to complete the NexSentry device configuration. A sample [nexsentr] screen follows:

```

1  [-----] NexSentry Device Configuration Entry
   Level  Name      Password      Report Definition
2  1  1  WPEP1  FAS01  2  Trigger : 1
3  2  F  WPEP2  FAS02  3  Time Code 1: 1
4  3  C  WPEP3  FAS03  4  Time Code 2: 1
5  4  I  WPEP4  FAS04  5  ABX Site Group : 1
6  5  E  WPEP5  FAS05  6  Auto Print : 0
7  6  -  -----  -----
8  7  -  -----  -----
9  8  -  -----  -----
10 9  -  -----  -----
11 10 8  WPEP8  FAS08  11  Time Code 4: 0
   11 11 11  WPEP11 FAS11  12  Time Code 3: 0
   12 12 12  WPEP12 FAS12  13  Time Code 4: 0
   13 13 13  WPEP13 FAS13  14  Time Code 1: 0
   14 14 14  WPEP14 FAS14  15  Time Code 2: 0
   15 15 15  WPEP15 FAS15  16  Time Code 3: 0
   16 16 16  WPEP16 FAS16  17  Time Code 4: 0
   17 17 17  WPEP17 FAS17  18  Time Code 1: 0
   18 18 18  WPEP18 FAS18  19  Time Code 2: 0
   19 19 19  WPEP19 FAS19  20  Time Code 3: 0
   20 20 20  WPEP20 FAS20  21  Time Code 4: 0
   21 21 21  WPEP21 FAS21  22  Time Code 1: 0
   22 22 22  WPEP22 FAS22  23  Time Code 2: 0
   23 23 23  WPEP23 FAS23  24  Time Code 3: 0
   24 24 24  WPEP24 FAS24  25  Time Code 4: 0
   25 25 25  WPEP25 FAS25  26  Time Code 1: 0
   26 26 26  WPEP26 FAS26  27  Time Code 2: 0
   27 27 27  WPEP27 FAS27  28  Time Code 3: 0
   28 28 28  WPEP28 FAS28  29  Time Code 4: 0
   29 29 29  WPEP29 FAS29  30  Time Code 1: 0
   30 30 30  WPEP30 FAS30  31  Time Code 2: 0
   31 31 31  WPEP31 FAS31  32  Time Code 3: 0
   32 32 32  WPEP32 FAS32  33  Time Code 4: 0
   33 33 33  WPEP33 FAS33  34  Time Code 1: 0
   34 34 34  WPEP34 FAS34  35  Time Code 2: 0
   35 35 35  WPEP35 FAS35  36  Time Code 3: 0
   36 36 36  WPEP36 FAS36  37  Time Code 4: 0
   37 37 37  WPEP37 FAS37  38  Time Code 1: 0
   38 38 38  WPEP38 FAS38  39  Time Code 2: 0
   39 39 39  WPEP39 FAS39  40  Time Code 3: 0
   40 40 40  WPEP40 FAS40  41  Time Code 4: 0
   41 41 41  WPEP41 FAS41  42  Time Code 1: 0
   42 42 42  WPEP42 FAS42  43  Time Code 2: 0
   43 43 43  WPEP43 FAS43  44  Time Code 3: 0
   44 44 44  WPEP44 FAS44  45  Time Code 4: 0
   45 45 45  WPEP45 FAS45  46  Time Code 1: 0
   46 46 46  WPEP46 FAS46  47  Time Code 2: 0
   47 47 47  WPEP47 FAS47  48  Time Code 3: 0
   48 48 48  WPEP48 FAS48  49  Time Code 4: 0
   49 49 49  WPEP49 FAS49  50  Time Code 1: 0
   50 50 50  WPEP50 FAS50  51  Time Code 2: 0
   51 51 51  WPEP51 FAS51  52  Time Code 3: 0
   52 52 52  WPEP52 FAS52  53  Time Code 4: 0
   53 53 53  WPEP53 FAS53  54  Time Code 1: 0
   54 54 54  WPEP54 FAS54  55  Time Code 2: 0
   55 55 55  WPEP55 FAS55  56  Time Code 3: 0
   56 56 56  WPEP56 FAS56  57  Time Code 4: 0
   57 57 57  WPEP57 FAS57  58  Time Code 1: 0
   58 58 58  WPEP58 FAS58  59  Time Code 2: 0
   59 59 59  WPEP59 FAS59  60  Time Code 3: 0
   60 60 60  WPEP60 FAS60  61  Time Code 4: 0
   61 61 61  WPEP61 FAS61  62  Time Code 1: 0
   62 62 62  WPEP62 FAS62  63  Time Code 2: 0
   63 63 63  WPEP63 FAS63  64  Time Code 3: 0
   64 64 64  WPEP64 FAS64  65  Time Code 4: 0
   65 65 65  WPEP65 FAS65  66  Time Code 1: 0
   66 66 66  WPEP66 FAS66  67  Time Code 2: 0
   67 67 67  WPEP67 FAS67  68  Time Code 3: 0
   68 68 68  WPEP68 FAS68  69  Time Code 4: 0
   69 69 69  WPEP69 FAS69  70  Time Code 1: 0
   70 70 70  WPEP70 FAS70  71  Time Code 2: 0
   71 71 71  WPEP71 FAS71  72  Time Code 3: 0
   72 72 72  WPEP72 FAS72  73  Time Code 4: 0
   73 73 73  WPEP73 FAS73  74  Time Code 1: 0
   74 74 74  WPEP74 FAS74  75  Time Code 2: 0
   75 75 75  WPEP75 FAS75  76  Time Code 3: 0
   76 76 76  WPEP76 FAS76  77  Time Code 4: 0
   77 77 77  WPEP77 FAS77  78  Time Code 1: 0
   78 78 78  WPEP78 FAS78  79  Time Code 2: 0
   79 79 79  WPEP79 FAS79  80  Time Code 3: 0
   80 80 80  WPEP80 FAS80  81  Time Code 4: 0
   81 81 81  WPEP81 FAS81  82  Time Code 1: 0
   82 82 82  WPEP82 FAS82  83  Time Code 2: 0
   83 83 83  WPEP83 FAS83  84  Time Code 3: 0
   84 84 84  WPEP84 FAS84  85  Time Code 4: 0
   85 85 85  WPEP85 FAS85  86  Time Code 1: 0
   86 86 86  WPEP86 FAS86  87  Time Code 2: 0
   87 87 87  WPEP87 FAS87  88  Time Code 3: 0
   88 88 88  WPEP88 FAS88  89  Time Code 4: 0
   89 89 89  WPEP89 FAS89  90  Time Code 1: 0
   90 90 90  WPEP90 FAS90  91  Time Code 2: 0
   91 91 91  WPEP91 FAS91  92  Time Code 3: 0
   92 92 92  WPEP92 FAS92  93  Time Code 4: 0
   93 93 93  WPEP93 FAS93  94  Time Code 1: 0
   94 94 94  WPEP94 FAS94  95  Time Code 2: 0
   95 95 95  WPEP95 FAS95  96  Time Code 3: 0
   96 96 96  WPEP96 FAS96  97  Time Code 4: 0
   97 97 97  WPEP97 FAS97  98  Time Code 1: 0
   98 98 98  WPEP98 FAS98  99  Time Code 2: 0
   99 99 99  WPEP99 FAS99  100 Time Code 3: 0
   100 100 100 WPEP100 FAS100 101 Time Code 4: 0
   101 101 101 WPEP101 FAS101 102 Time Code 1: 0
   102 102 102 WPEP102 FAS102 103 Time Code 2: 0
   103 103 103 WPEP103 FAS103 104 Time Code 3: 0
   104 104 104 WPEP104 FAS104 105 Time Code 4: 0
   105 105 105 WPEP105 FAS105 106 Time Code 1: 0
   106 106 106 WPEP106 FAS106 107 Time Code 2: 0
   107 107 107 WPEP107 FAS107 108 Time Code 3: 0
   108 108 108 WPEP108 FAS108 109 Time Code 4: 0
   109 109 109 WPEP109 FAS109 110 Time Code 1: 0
   110 110 110 WPEP110 FAS110 111 Time Code 2: 0
   111 111 111 WPEP111 FAS111 112 Time Code 3: 0
   112 112 112 WPEP112 FAS112 113 Time Code 4: 0
   113 113 113 WPEP113 FAS113 114 Time Code 1: 0
   114 114 114 WPEP114 FAS114 115 Time Code 2: 0
   115 115 115 WPEP115 FAS115 116 Time Code 3: 0
   116 116 116 WPEP116 FAS116 117 Time Code 4: 0
   117 117 117 WPEP117 FAS117 118 Time Code 1: 0
   118 118 118 WPEP118 FAS118 119 Time Code 2: 0
   119 119 119 WPEP119 FAS119 120 Time Code 3: 0
   120 120 120 WPEP120 FAS120 121 Time Code 4: 0
   121 121 121 WPEP121 FAS121 122 Time Code 1: 0
   122 122 122 WPEP122 FAS122 123 Time Code 2: 0
   123 123 123 WPEP123 FAS123 124 Time Code 3: 0
   124 124 124 WPEP124 FAS124 125 Time Code 4: 0
   125 125 125 WPEP125 FAS125 126 Time Code 1: 0
   126 126 126 WPEP126 FAS126 127 Time Code 2: 0
   127 127 127 WPEP127 FAS127 128 Time Code 3: 0
   128 128 128 WPEP128 FAS128 129 Time Code 4: 0
   129 129 129 WPEP129 FAS129 130 Time Code 1: 0
   130 130 130 WPEP130 FAS130 131 Time Code 2: 0
   131 131 131 WPEP131 FAS131 132 Time Code 3: 0
   132 132 132 WPEP132 FAS132 133 Time Code 4: 0
   133 133 133 WPEP133 FAS133 134 Time Code 1: 0
   134 134 134 WPEP134 FAS134 135 Time Code 2: 0
   135 135 135 WPEP135 FAS135 136 Time Code 3: 0
   136 136 136 WPEP136 FAS136 137 Time Code 4: 0
   137 137 137 WPEP137 FAS137 138 Time Code 1: 0
   138 138 138 WPEP138 FAS138 139 Time Code 2: 0
   139 139 139 WPEP139 FAS139 140 Time Code 3: 0
   140 140 140 WPEP140 FAS140 141 Time Code 4: 0
   141 141 141 WPEP141 FAS141 142 Time Code 1: 0
   142 142 142 WPEP142 FAS142 143 Time Code 2: 0
   143 143 143 WPEP143 FAS143 144 Time Code 3: 0
   144 144 144 WPEP144 FAS144 145 Time Code 4: 0
   145 145 145 WPEP145 FAS145 146 Time Code 1: 0
   146 146 146 WPEP146 FAS146 147 Time Code 2: 0
   147 147 147 WPEP147 FAS147 148 Time Code 3: 0
   148 148 148 WPEP148 FAS148 149 Time Code 4: 0
   149 149 149 WPEP149 FAS149 150 Time Code 1: 0
   150 150 150 WPEP150 FAS150 151 Time Code 2: 0
   151 151 151 WPEP151 FAS151 152 Time Code 3: 0
   152 152 152 WPEP152 FAS152 153 Time Code 4: 0
   153 153 153 WPEP153 FAS153 154 Time Code 1: 0
   154 154 154 WPEP154 FAS154 155 Time Code 2: 0
   155 155 155 WPEP155 FAS155 156 Time Code 3: 0
   156 156 156 WPEP156 FAS156 157 Time Code 4: 0
   157 157 157 WPEP157 FAS157 158 Time Code 1: 0
   158 158 158 WPEP158 FAS158 159 Time Code 2: 0
   159 159 159 WPEP159 FAS159 160 Time Code 3: 0
   160 160 160 WPEP160 FAS160 161 Time Code 4: 0
   161 161 161 WPEP161 FAS161 162 Time Code 1: 0
   162 162 162 WPEP162 FAS162 163 Time Code 2: 0
   163 163 163 WPEP163 FAS163 164 Time Code 3: 0
   164 164 164 WPEP164 FAS164 165 Time Code 4: 0
   165 165 165 WPEP165 FAS165 166 Time Code 1: 0
   166 166 166 WPEP166 FAS166 167 Time Code 2: 0
   167 167 167 WPEP167 FAS167 168 Time Code 3: 0
   168 168 168 WPEP168 FAS168 169 Time Code 4: 0
   169 169 169 WPEP169 FAS169 170 Time Code 1: 0
   170 170 170 WPEP170 FAS170 171 Time Code 2: 0
   171 171 171 WPEP171 FAS171 172 Time Code 3: 0
   172 172 172 WPEP172 FAS172 173 Time Code 4: 0
   173 173 173 WPEP173 FAS173 174 Time Code 1: 0
   174 174 174 WPEP174 FAS174 175 Time Code 2: 0
   175 175 175 WPEP175 FAS175 176 Time Code 3: 0
   176 176 176 WPEP176 FAS176 177 Time Code 4: 0
   177 177 177 WPEP177 FAS177 178 Time Code 1: 0
   178 178 178 WPEP178 FAS178 179 Time Code 2: 0
   179 179 179 WPEP179 FAS179 180 Time Code 3: 0
   180 180 180 WPEP180 FAS180 181 Time Code 4: 0
   181 181 181 WPEP181 FAS181 182 Time Code 1: 0
   182 182 182 WPEP182 FAS182 183 Time Code 2: 0
   183 183 183 WPEP183 FAS183 184 Time Code 3: 0
   184 184 184 WPEP184 FAS184 185 Time Code 4: 0
   185 185 185 WPEP185 FAS185 186 Time Code 1: 0
   186 186 186 WPEP186 FAS186 187 Time Code 2: 0
   187 187 187 WPEP187 FAS187 188 Time Code 3: 0
   188 188 188 WPEP188 FAS188 189 Time Code 4: 0
   189 189 189 WPEP189 FAS189 190 Time Code 1: 0
   190 190 190 WPEP190 FAS190 191 Time Code 2: 0
   191 191 191 WPEP191 FAS191 192 Time Code 3: 0
   192 192 192 WPEP192 FAS192 193 Time Code 4: 0
   193 193 193 WPEP193 FAS193 194 Time Code 1: 0
   194 194 194 WPEP194 FAS194 195 Time Code 2: 0
   195 195 195 WPEP195 FAS195 196 Time Code 3: 0
   196 196 196 WPEP196 FAS196 197 Time Code 4: 0
   197 197 197 WPEP197 FAS197 198 Time Code 1: 0
   198 198 198 WPEP198 FAS198 199 Time Code 2: 0
   199 199 199 WPEP199 FAS199 200 Time Code 3: 0
   200 200 200 WPEP200 FAS200 201 Time Code 4: 0
   201 201 201 WPEP201 FAS201 202 Time Code 1: 0
   202 202 202 WPEP202 FAS202 203 Time Code 2: 0
   203 203 203 WPEP203 FAS203 204 Time Code 3: 0
   204 204 204 WPEP204 FAS204 205 Time Code 4: 0
   205 205 205 WPEP205 FAS205 206 Time Code 1: 0
   206 206 206 WPEP206 FAS206 207 Time Code 2: 0
   207 207 207 WPEP207 FAS207 208 Time Code 3: 0
   208 208 208 WPEP208 FAS208 209 Time Code 4: 0
   209 209 209 WPEP209 FAS209 210 Time Code 1: 0
   210 210 210 WPEP210 FAS210 211 Time Code 2: 0
   211 211 211 WPEP211 FAS211 212 Time Code 3: 0
   212 212 212 WPEP212 FAS212 213 Time Code 4: 0
   213 213 213 WPEP213 FAS213 214 Time Code 1: 0
   214 214 214 WPEP214 FAS214 215 Time Code 2: 0
   215 215 215 WPEP215 FAS215 216 Time Code 3: 0
   216 216 216 WPEP216 FAS216 217 Time Code 4: 0
   217 217 217 WPEP217 FAS217 218 Time Code 1: 0
   218 218 218 WPEP218 FAS218 219 Time Code 2: 0
   219 219 219 WPEP219 FAS219 220 Time Code 3: 0
   220 220 220 WPEP220 FAS220 221 Time Code 4: 0
   221 221 221 WPEP221 FAS221 222 Time Code 1: 0
   222 222 222 WPEP222 FAS222 223 Time Code 2: 0
   223 223 223 WPEP223 FAS223 224 Time Code 3: 0
   224 224 224 WPEP224 FAS224 225 Time Code 4: 0
   225 225 225 WPEP225 FAS225 226 Time Code 1: 0
   226 226 226 WPEP226 FAS226 227 Time Code 2: 0
   227 227 227 WPEP227 FAS227 228 Time Code 3: 0
   228 228 228 WPEP228 FAS228 229 Time Code 4: 0
   229 229 229 WPEP229 FAS229 230 Time Code 1: 0
   230 230 230 WPEP230 FAS230 231 Time Code 2: 0
   231 231 231 WPEP231 FAS231 232 Time Code 3: 0
   232 232 232 WPEP232 FAS232 233 Time Code 4: 0
   233 233 233 WPEP233 FAS233 234 Time Code 1: 0
   234 234 234 WPEP234 FAS234 235 Time Code 2: 0
   235 235 235 WPEP235 FAS235 236 Time Code 3: 0
   236 236 236 WPEP236 FAS236 237 Time Code 4: 0
   237 237 237 WPEP237 FAS237 238 Time Code 1: 0
   238 238 238 WPEP238 FAS238 239 Time Code 2: 0
   239 239 239 WPEP239 FAS239 240 Time Code 3: 0
   240 240 240 WPEP240 FAS240 241 Time Code 4: 0
   241 241 241 WPEP241 FAS241 242 Time Code 1: 0
   242 242 242 WPEP242 FAS242 243 Time Code 2: 0
   243 243 243 WPEP243 FAS243 244 Time Code 3: 0
   244 244 244 WPEP244 FAS244 245 Time Code 4: 0
   245 245 245 WPEP245 FAS245 246 Time Code 1: 0
   246 246 246 WPEP246 FAS246 247 Time Code 2: 0
   247 247 247 WPEP247 FAS247 248 Time Code 3: 0
   248 248 248 WPEP248 FAS248 249 Time Code 4: 0
   249 249 249 WPEP249 FAS249 250 Time Code 1: 0
   250 250 250 WPEP250 FAS250 251 Time Code 2: 0
   251 251 251 WPEP251 FAS251 252 Time Code 3: 0
   252 252 252 WPEP252 FAS252 253 Time Code 4: 0
   253 253 253 WPEP253 FAS253 254 Time Code 1: 0
   254 254 254 WPEP254 FAS254 255 Time Code 2: 0
   255 255 255 WPEP255 FAS255 256 Time Code 3: 0
   256 256 256 WPEP256 FAS256 257 Time Code 4: 0
   257 257 257 WPEP257 FAS257 258 Time Code 1: 0
   258 258 258 WPEP258 FAS258 259 Time Code 2: 0
   259 259 259 WPEP259 FAS259 260 Time Code 3: 0
   260 260 260 WPEP260 FAS260 261 Time Code 4: 0
   261 261 261 WPEP261 FAS261 262 Time Code 1: 0
   262 262 262 WPEP262 FAS262 263 Time Code 2: 0
   263 263 263 WPEP263 FAS263 264 Time Code 3: 0
   264 264 264 WPEP264 FAS264 265 Time Code 4: 0
   265 265 265 WPEP265 FAS265 266 Time Code 1: 0
   266 266 266 WPEP266 FAS266 267 Time Code 2: 0
   267 267 267 WPEP267 FAS267 268 Time Code 3: 0
   268 268 268 WPEP268 FAS268 269 Time Code 4: 0
   269 269 269 WPEP269 FAS269 270 Time Code 1: 0
   270 270 270 WPEP270 FAS270 271 Time Code 2: 0
   271 271 271 WPEP271 FAS271 272 Time Code 3: 0
   272 272 272 WPEP272 FAS272 273 Time Code 4: 0
   273 273 273 WPEP273 FAS273 274 Time Code 1: 0
   274 274 274 WPEP274 FAS274 275 Time Code 2: 0
   275 275 275 WPEP275 FAS275 276 Time Code 3: 0
   276 276 276 WPEP276 FAS276 277 Time Code 4: 0
   277 277 277 WPEP277 FAS277 278 Time Code 1: 0
   278 278 278 WPEP278 FAS278 279 Time Code 2: 0
   279 279 279 WPEP279 FAS279 280 Time Code 3: 0
   280 280 280 WPEP280 FAS280 281 Time Code 4: 0
   281 281 281 WPEP281 FAS281 282 Time Code 1: 0
   282 282 282 WPEP282 FAS282 283 Time Code 2: 0
   283 283 283 WPEP283 FAS283 284 Time Code 3: 0
   284 284 284 WPEP284 FAS284 285 Time Code 4: 0
   285 285 285 WPEP285 FAS285 286 Time Code 1: 0
   286 286 286 WPEP286 FAS286 287 Time Code 2: 0
   287 287 287 WPEP287 FAS287 288 Time Code 3: 0
   288 288 288 WPEP288 FAS288 289 Time Code 4: 0
   289 289 289 WPEP289 FAS289 290 Time Code 1: 0
   290 290 290 WPEP290 FAS290 291 Time Code 2: 0
   291 291 291 WPEP291 FAS291 292 Time Code 3: 0
   292 292 292 WPEP292 FAS292 293 Time Code 4: 0
   293 293 293 WPEP293 FAS293 294 Time Code 1: 0
   294 294 294 WPEP294 FAS294 295 Time Code 2: 0
   295 295 295 WPEP295 FAS295 296 Time Code 3: 0
   296 296 296 WPEP296 FAS296 297 Time Code 4: 0
   297 297 297 WPEP297 FAS297 298 Time Code 1: 0
   298 298 298 WPEP298 FAS298 299 Time Code 2: 0
   299 299 299 WPEP299 FAS299 300 Time Code 3: 0
   300 300 300 WPEP300 FAS300 301 Time Code 4: 0
   301 301 301 WPEP301 FAS301 302 Time Code 1: 0
   302 302 302 WPEP302 FAS302 303 Time Code 2: 0
   303 303 303 WPEP303 FAS303 304 Time Code 3: 0
   304 304 304 WPEP304 FAS304 305 Time Code 4: 0
   305 305 305 WPEP305 FAS305 306 Time Code 1: 0
   306 306 306 WPEP306 FAS306 307 Time Code 2: 0
   307 307 307 WPEP307 FAS307 308 Time Code 3: 0
   308 308 308 WPEP308 FAS308 309 Time Code 4: 0
   309 309 309 WPEP309 FAS309 310 Time Code 1: 0
   310 310 310 WPEP310 FAS310 311 Time Code 2: 0
   311 311 311 WPEP311 FAS311 312 Time Code 3: 0
   312 312 312 WPEP312 FAS312 313 Time Code 4: 0
   313 313 313 WPEP313 FAS313 314 Time Code 1: 0
   314 314 314 WPEP314 FAS314 315 Time Code 2: 0
   315 315 315 WPEP315 FAS315 316 Time Code 3: 0
   316 316 316 WPEP316 FAS316 317 Time Code 4: 0
   317 317 317 WPEP317 FAS317 318 Time Code 1: 0
   318 318 318 WPEP318 FAS318 319 Time Code 2: 0
   319 319 319 WPEP319 FAS319 320 Time Code 3: 0
   320 320 320 WPEP320 FAS320 321 Time Code 4: 0
   321 321 321 WPEP321 FAS321 322 Time Code 1: 0
   322 322 322 WPEP322 FAS322 323 Time Code 2: 0
   323 323 323 WPEP323 FAS323 324 Time Code 3: 0
   324 324 324 WPEP324 FAS324 325 Time Code 4: 0
   325 325 325 WPEP325 FAS325 326 Time Code 1: 0
   326 326 326 WPEP326 FAS326 327 Time Code 2: 0
   327 327 327 WPEP327 FAS327 328 Time Code 3: 0
   328 328 328 WPEP328 FAS328 329 Time Code 4: 0
   329 329 329 WPEP329 FAS329 330 Time Code 1: 0
   330 330 330 WPEP330 FAS330 331 Time Code 2: 0
   331 331 331 WPEP331 FAS331 332 Time Code 3: 0
   332 332 332 WPEP332 FAS332 333 Time Code 4: 0
   333 333 333 WPEP333 FAS333 334 Time Code 1: 0
   334 334 334 WPEP334 FAS334 335 Time Code 2: 0
   335 335 335 WPEP335 FAS335 336 Time Code 3: 0
   336 336 336 WPEP336 FAS336 337 Time Code 4: 0
   337 337 337 WPEP337 FAS337 338 Time Code 1: 0
   338 338 338 WPEP338 FAS338 339 Time Code 2: 0
   339 339 339 WPEP339 FAS339 340 Time Code 3: 0
   340 340 340 WPEP340 FAS340 341 Time Code 4: 0
   341
```

**NOTE**

The *Level*, *Name* and *Password* fields are specific to the NexSentry and applies only to operators logging in directly via the ACU's terminal port. The fields are not part of the SE 6000 control parameters.

**Tamper.** Optional. Enter the tamper report number if a report has been created (see applicable ACU manual). The report states the system actions that will be taken if the ACU enclosure housing is opened. Default is 0.

- ③ **Power Fail.** Optional. Enter the power fail report number if a report has been created (see applicable ACU manual). The report states the actions that will be taken by the ACU should a power failure occur. Default is 0.
- ④ **Override.** Optional. Enter the operator override report number if a report has been created (see applicable ACU manual). The report states the actions that will be taken by the ACU if, for example, a manual unlock or a shunt occurs. Default is 0.
- ⑤ **ABA Site Group.** Optional. The ABA site code group ID number.
- ⑥ **Auto Forgive.** Optional. Up to four time codes can be entered that execute the forgive command at the ACU. Default is 0 (feature disabled if all auto-forgive time codes are 0).
- ⑦ **808 Modem Definition.** Not used.
- ⑧ **Number of Retry Times.** Not used.
- ⑨ **XON/XOFF.** Not used.
- ⑩ **Building Closed Time Codes.** Optional. Provides up to four time intervals during which the building should be closed. Default is 0.

**Building Open Reminder.** Optional. If the building should be closed (indicated by the time codes entered in the previous field), a reminder message is logged and repeated the number of minutes specified (0 to 240). Default is 0.

## SE 818 DEVICE CONFIGURATION ENTRY [d818entr]

Complete the [d818entr] screen for all 818-series and NexSentry ACUs (use F2 to display the screen after the previous screen, [d808entr] or [nexsentr], have been stored). A sample screen follows:

```

[d818entr]      818 Device Configuration Entry ( Page [ ] )
1 PIN Seed      : 0           5 Max PIN Retries: 4
2 Duress PIN Digits : 0       6 VIP Only Digits: 4
3 Print PIN's    : Y         7 Duress Report  : 0
4 PIN Timeout   : 10        8 Duress Enable  : Y

```

**PIN Seed.** Optional. Enter the base seed number for generating PINs. The value entered has priority over the system default PIN seed value entered with the [pndfentr] screen (see *SE 422 Pin Definition* in this section). Default is 0.

**Duress PIN Digits.** Optional. Enter the allowed number of digits for a PIN duress code. Default is 0.

3 **Print PINs.** Optional. A Y/N field indicating if the PIN should be displayed once calculated. Default is Y.

4 **PIN Timeout.** Optional. Enter the maximum number of seconds allowed between key presentation and PIN entry. Default is 10.

5 **Max PIN Retries.** Optional. Enter the allowed number of PIN entry retries. Default is 4.

6 **VIP Only Digits.** Optional for keypad-controlled doors only. Enter the allowed number of digits for the PIN (4—8). Default is 4.

7 **Duress Report.** Optional. Enter an action report number (1—32) indicating the action the ACU is to take should a duress event occur. Default is 0.

8 **Duress Enable.** Optional. A Y/N field indicating whether the duress feature is enabled. Default is Y.

## SE 422 DEVICE CONFIGURATION ENTRY [d422entr]

Complete the [d422entr] screen for SE 422 ACUs (use F2 to display the screen after the previous screen has been stored). A sample screen follows:

```

ld422enlr]          SE/422 Device Configuration Entry
  Level  Name      Password      Report Definition
1>  1  OPER1      MASTEROP    2 Duress      : 1
2>  2  PEGGY      PEGPAS      3 System      : 1
3>  3  SANDRINGHAM  PROGRAM     4 Op Override: 1
4>  4  GOWERS      GOGOWRS
5>  5  GUARD1      GD1         5 Alarm Delay: 5
6>  6  GUARD2      GD2         6 PIN Timeout: 10
7>  7  GUARD3      GD3         7 Max Inu. PIN's: 4
8>  8  OPERTEMP    OPTMP       8 VIP's Digits: 4
9 422 Modem Definition: 10 Latched Contact: 1

11 ABA Site Code Grp: 1
12 EMPI Alt1 Code: 0
13 PIN Seed: 5526 14 PIN Digits: 4 15 EMPI Alt2 Code: 0
16 Number Of Retry Times: 3 17 XON/XOFF: Term Port 18 Bldg Mode Indicators
19 Duress Enable: 20 Show PIN: Y Host Port N Monitor B Limited B
Building Closed Times: Tncd1: B Tncd2: B Open B Closed B
Tncd3: B Tncd4: B Building Open Reminder: B

```

**Level, Name, Password.** Required. These first three fields are entered to identify up to eight operators who will be permitted to set / change system parameters for this particular ACU. User 1 must be established (defaults to operator 1); operators 2 through 7 are optional. Enter the operator's security code (A through F), name and password.

The security codes A through F control the degree to which the operator may add/change/delete the system parameters. Code A has the most privileges, code F has the least. For detailed information concerning operator privilege levels, refer to the applicable ACU manual.

#### NOTE

The *Level*, *Name* and *Password* fields are specific to individual SE 422s and apply only to operators logging in directly via the ACU's terminal port. The fields are not part of the SE 6000 control parameters.

**Duress.** Optional. A number (1-32) which instructs the SE 422 which action report to use should a duress event occur. Default is 1.

**3 System.** Optional. A number (1-32) which instructs the SE 422 which action report to use in response to system events in the SE 422. Default is 1.

**4 Op. Override.** Optional. A number (1-32) which instructs the SE 422 which action report to use in response to operator overrides performed on the SE 422. Default is 1.

**5 Alarm Delay.** Optional. The amount of time in seconds (10-240) that an alarm condition is allowed to exist before the alarm contact is closed. Default is 30.

- 
- ⑥ **PIN Timeout.** Optional. The maximum amount of time, in seconds, which can pass between the presentation of a key and the entry of a verification PIN. Default is 10.
  - ⑦ **Max Inv. PINs.** Optional. The maximum number of invalid PIN entry attempts to permit before cancelling the key presentation. Default is 4.
  - ⑧ **VIPs Digits.** Optional. The number of digits in the PIN number for doors using keypads only. The range is 4 to 8. Default is 4.
  - ⑨ **Modem Definition.** Not used when the SE 6000 is connected directly or in a dial-up configuration.
  - ⑩ **Latched Contact.** Optional. The number of the output contacts that are assigned as a latched contact (0—51). Default is 0.  
  
**ABA Site Code Grp.** Optional. The ABA site code group ID number.
  - ⑫ **EMPI Alt1 Code.** Optional. Alternate EMPI site code #1.
  - ⑬ **PIN seed.** Optional. The base seed number used when generating PINs. The value entered here has priority over the default PIN seed value entered on the [pndfentr] screen (see *Entering Default PIN Digits and Seed for an SE 422* in this section). Default is 0.
  - ⑭ **PIN Digits.** The number of digits in the PIN code for this SE 422. The value entered here has priority over the default PIN digits value entered on the [pndfentr] screen (see *Entering Default PIN Digits and Seed for an SE 422* in this section). Default is 0.
  - ⑮ **EMPI Alt2 Code.** Optional. Alternate EMPI site code #2.
  - ⑯ **# of Retry Times.** Used to inform a remotely connected SE 422 the number of times to attempt to contact the host computer over telephone lines before considering a connection to be currently impossible to make.
  - ⑰ **XON/XOFF.** Terminal Port and Host Port: Used to inform the SE 422 whether XON/XOFF flow control will be used at either of these two ports. Used for remotely connected SE 422s only.
  - ⑱ **Bldg Mode Indicators.** Conditional. Enter the input point contact number or output relay number to initiate and display the status of the building mode.

Monitor — Input point contact ID (0 — 75)

Open, Limited, Closed — Output point relay ID (0 — 51)

---

- 19 **Duress Enable.** Indicates with a Y or an N whether the PIN duress feature of the SE 422 is turned on or not.
- 20 **Show PIN.** Indicates with a Y or an N whether the PIN number should be displayed on a local terminal connected to the SE 422 after it has been calculated.

**Building Closed Times.** Enter up to four time codes used for building closure.

**Building Open Reminder.** Enter the number of seconds (0 — 240) that the building open message is to display.

## READERS

Readers are usually assigned to ACUs, but they may be used as standalone devices or linked to other security monitoring devices. Twelve reader types (1 — 12) are currently defined:

1. **Access Control.** Controls power to a door lock allowing or denying entry.
2. **Time and Attendance** (optional feature). Monitors keyholders' entry/exit movements.
3. **Meal Monitoring** (optional feature). Tracks number of meals taken by a keyholder.
4. **Guard Tour** (optional feature). Monitors guard check-in activities during guard rounds.
5. **Elevator Control.** Controls and limits keyholder access to floors.
6. **Activate** (optional feature). Enables keys for system wide use.
7. **Deactivate** (optional feature). Disables previously activated keys (see previous item).
8. **Auto Key Entry.** Allows automatic entry of card numbers.
9. **Access with Keypad.** Same as #1 except that a keypad is used in addition to the reader.
10. **Keypad.** Keypad only.
11. **Access with Two-Man Rule.** (optional feature). Same as #1 above except that two-man rule is in effect.
12. **MultiOcc Reader.** Multiple occupancy reader. Similar to #11 except that it requires that two keyholders enter and leave a zone together. Refer to the subsection that covers multiple occupancy readers in this section for more details.

Data entry begins with the [rdr\_entr] screen. (One additional screen each is used for readers assigned to SE NexSentry, 8xx series, and 422 ACUs. Details follow this subsection.)

## READER ENTRY [rdr\_entr]

```

[1] (rdr_entr)                               [2] Reader Entry
[3] Reader ID: 1001                          [2] Reader Description: 422 ENTRY #1
[3] Device ID: 100 = DIAL-UP 422 #1
[3] (Computer ID: 100 Poller : 0 Address: 1 ) [4] Sensor: 1
[5] Enable Point ID: 0 =
[6] Reader Type : 1 = Access Control          [7] Assoc Reader ID: 1002
[8] Door Switch ID : 100 = 422 1001 DR SU (1.0) [9] Trace: N [10] Disable: N
[11] Hex Point ID : 109 = 422 1001 REX (1.1)
[12] TSA Dir: [13] Unlock Time: 15 [14] Read While Open: [15] Reverse Lock: N
[16] Entering Zone : 0 = ALL ZONES
[17] Leaving Zone : 0 = ALL ZONES
[18] Tenant : 0 = ALL ENCOMPASSING
[19]
Mod Start End Mon Tue Wed Thu Fri Sat Sun Hol
Tr Cd 1: 1 0 00:00 - 23:59 - Y Y Y Y Y Y Y Y
Tr Cd 2: 0 0 00:00 - 00:00 - N N N N N N N N
Tr Cd 3: 0 0 00:00 - 00:00 - N N N N N N N N
Tr Cd 4: 0 0 00:00 - 00:00 - N N N N N N N N

PRESS <F2> TO CREATE REPORT DEFINITIONS FOR 800S DEVICES ONLY

```

**Reader ID.** Required (*zoom* available). Enter a maximum four-digit reader ID number.

**Reader Description.** Optional. Enter a maximum 20-character description of the reader. Default is the reader ID number.

- 3 Device ID.** Required (*zoom* available). Enter the number of the device which controls this reader. The related information (computer ID, poller number, address) automatically displays when the ID is entered.
- 4 Sensor.** Required. Enter the sensor port number of the ACU to which this reader is connected.
- 5 Enable Point ID.** Conditional (*zoom* available). Indicates a point ID that must be activated before the current point can be activated. Enter the enable point ID number.

**NOTE**

The **Enable Point** is primarily used with closed circuit television monitors, but can be used elsewhere. For example, a guard might need to personally recognize you and press an OK button (activates enable point) before your card will work at an ACU (current point). The system enters the default value of 0 (zero) if this field does not apply.

- 
- ⑥ **Reader Type.** Required. Enter the reader type number in the ranges 1 through 12 as described above.
  - ⑦ **Assoc Reader ID (Associated Reader).** Required if the reader is used in conjunction with a keypad. Enter the ID number of the Reader used with the keypad. Default is 0.
  - ⑧ **Door Switch ID.** Required. Enter the door switch point ID used in conjunction with this reader. (If passback protection is in effect, two readers may share a single door switch.) The system enters the default value of 0 (zero) if this field does not apply.
  - ⑨ **Trace.** A Y/N field used to indicate if all events at this reader are to be specially reported (traced). Default is N.
  - ⑩ **Disable.** Required. A Y/N field indicating if the device is to be shunted at system start up (Y). This function varies with different types of ACUs. Default is N (device not shunted).  
  
**REX Point ID.** Required if the reader is used in conjunction with a request-to-exit (REX) device or switch. Enter the REX ID number. The system enters the default value of 0 (zero) if this field does not apply.
  - ⑫ **T & A Dir.** Time and attendance direction. If the time and attendance feature is used, enter N—None, I—Global In, or O—Global Out. The default is N.
  - ⑬ **Unlock Time.** Optional for NexSentry, 8xx-series, and SE 422 ACUs. Enter a time period in seconds (1-240) that the door is to remain unlocked when a valid key is presented. Default is 10 seconds.
  - ⑭ **Read While Open.** Optional for NexSentry, 8xx-series, and SE 422 ACUs. A Y/N field used to indicate if keys are to be read while the door is unlocked. The default is N.
  - ⑮ **Reverse Lock.** Optional for NexSentry, 8xx-series, and SE 422 ACUs. A Y/N field used to indicate if the lock power is normally off (N) or on (Y).
  - ⑯ **Entering Zone.** Optional. Enter the zone number for this reader, if applicable.
  - ⑰ **Leaving Zone.** Optional. Used with anti-passback if reader controls exit from a zone. Enter the exit zone number.
  - ⑱ **Tenant.** Optional. Enter a four-digit maximum tenant number. If omitted, Tenant 0 (zero - system owner) is entered by default.
  - ⑲ **Tim Cd 1: ... and Mod.** Both optional. Four time codes may be entered denoting when this reader is active This function varies with different types of ACUs. Note that the downloaded ACU will still operate in the field during excluded time periods. If omitted, the reader is never
-

active. For **Mod**, enter a transaction modifier code (A, B, etc.) to customize log messages and system actions (see *Section 6: System Administration* for details). The default for Mod is 0 (zero); use the standard log message.

## **AUTO KEY ENTRY AND READER**

The Auto Key Entry feature allows you to capture the key number from a key card and assign the number as well as enter the card number automatically in the Key Number field of the keyholder Entry [key\_entr] screen. Before you can use this feature you must configure an Auto-Entry Reader (Reader type 8). Perform the following procedures:

- Configuring the Auto-Entry Reader
- Automatically Entering Card Numbers

### **Configuring the Auto Entry Reader**

1. From the Main Menu, select Master File Entry and the Master File Entry screen appears.
2. Select the Hardware Configuration menu and the Configuration Menu [confmenu] screen appears.
3. Select Readers and the Reader Entry [rdr\_entr] screen appears.
4. Select F5 Add Mode.
5. Enter all necessary information, making sure that you enter 8 in the Reader Type field.
6. Select F6 Store.

### **Automatically Entering Card Numbers**

Note before you use the following procedure, you should configure an Auto-Entry Reader.

1. From the Main Menu, select Master File Entry and the Master File Entry screen appears.
2. Select Keyholders and the Keyholder Entry [key\_entr] screen appears.
3. Select F5 Add Mode.
4. Enter the keyholders's ID, Last name, and first name and press Enter after each entry.
5. Position the key card next to the reader and at the beep, press F7 AutoKey.
6. Select F6 Store and select F5 Add Mode to enter additional Keyholders.
7. To enter additional keyholders, repeat steps 4 through 6.

## **MULTIPLE OCCUPANCY READER**

The Multiple Occupancy Reader (MOR) is similar to a reader that is configured for the two-man rule requirement. The difference between them is that the multiple occupancy reader is also

---

configured for a specific zone and includes the passback feature. In addition, the MOR and the SE 6000 keep track of the people that are in a specified zone.

### ENTERING A MULTIPLE OCCUPANCY ZONE

When a multiple occupancy zone is vacant, two keyholders are required to present their keys to the reader to unlock the door; first one and within a prescribed time period, the other, unlocking the door. Once three or more people are in the multiple occupancy zone, the reader works like a standard reader, that is, as an individual keyholder with rights presents their key, the door is unlocked, either entering or leaving.

### VACATING A MULTIPLE OCCUPANCY ZONE

Vacating a Multiple Occupancy zone, requires that the last two keyholders present their keys at the same time, first one and then within the prescribed time period the other, unlocking the door.

### READER REPORT DEFINITION SCREENS

The reader report definition screens, [rdr1entr], [rdr2entr], [rdr3entr], and [rdr4entr] are used, respectively, when setting up a reader to operate with an SE 8xx-series, 422, or NexSentry ACU. Press F2 after storing the data on the [rdr\_entr] screen; the appropriate second screen automatically displays.

### SE 8XX-SERIES READER REPORT DEFINITION [rdr1entr]

| [rdr1entr] |                | 888 Reader Report Definition |                      |
|------------|----------------|------------------------------|----------------------|
| 1          | Reader Mode    | 3                            |                      |
|            | Forced Open    | 1                            | Door Open Too Long 1 |
|            | Access Granted | 2                            | Access Denied 1      |
|            | Coax Failure   | 1                            | Sensor Failure 1     |
|            | Key Trace      | 2                            | Msm Failure 1        |
|            | Exit Granted   | 1                            | Exit Denied 1        |

**Reader Mode.** Optional. Enter the appropriate reader mode number. This is used for building modes. The default is 0.

0 = Normal, 1 = Open, 2 = Closed, 3 = Station

The remaining fields, *Forced Open* through *Exit Denied*, require a report number entry. The word report in this context identifies a user-defined action or series of actions that the ACU is to take

in response to various events occurring within the system. (The field titles indicate the event types.) See *Device Report Definition* in the section and the applicable ACU manual for detailed information.

### SE 422 READER REPORT DEFINITION [rdr2entr]

| Lrdr2entrJ |                                      | SE/422 Reader Report Definition |      |      |                           |        |
|------------|--------------------------------------|---------------------------------|------|------|---------------------------|--------|
| 1          | Reader Mode                          | :                               | 3    |      |                           |        |
| 2          | Proximity Type                       | :                               | 0    | 3    | Proximity Code : 0        |        |
| 4          | Keypad Type                          | :                               | 0    | 5    | Keypad Code : 0           |        |
| 6          | Mag Stripe Type                      | :                               | 0    | 7    | Mag Stripe Code : 0       |        |
| 8          | Forced Open                          | :                               | 1    | 9    | Door Open Too Long: 1     |        |
| 10         | Access Granted                       | :                               | 1    | 11   | Access Denied : 1         |        |
| 12         | Key Trace                            | :                               | 1    | 13   | Exit Denied : 1           |        |
| 14         | Exit Granted                         | :                               | 1    | 15   | Door Output Relay : 00    |        |
| 16         | DKA Configuration                    | :                               | 0    | 17   | ABA Configuration : ***** |        |
| 18         | Keypad Enable:                       |                                 | N    | Open | Limited                   | Closed |
| 19         | Keypad Active During Building Modes: |                                 | N    | N    | N                         | N      |
| 20         | Keypad Active During Timecodes:      |                                 | 1> 0 | 2> 0 | 3> 0                      | 4> 0   |

**Reader Mode.** Optional. Enter the appropriate reader mode number: 0 = Normal, 1 = Open, 2 = Closed, 3 = Station. Default is 0.

**Proximity Type.** Enter the proximity type: 0 = Sensor interface, 1 = DigiKey reader.

- 3 **Proximity Code.** Enter the proximity reader node number: 0 = None, 15 = 1st proximity reader node number, 16 = 2nd proximity reader node number
- 4 **Keypad Type.** Enter the keypad type: 0 = VIP2, 1 = MSR5.
- 5 **Keypad Code.** Enter the node number for the VIP keypad: 0 = None, 13 = 1st keypad node number, 14 = 2nd keypad node number.
- 6 **Mag Stripe Type.** Enter the magnetic stripe type: 0 = MSR, 1 = MSR5, 2 = MSR5.
- 7 **Mag Stripe Code.** Enter the node number for the magnetic stripe reader: 0 = None, 17 = 1st magnetic stripe reader node number, 18 = 2nd magnetic stripe reader node number.

**8—14**

The following ten fields, **Forced Open** through **Exit Granted**, require the entry of a report number. The word report in this context identifies a user-defined action or series of actions that the ACU is to take in response to various events occurring within the system. (The field titles indicate the event types.) See *Device Report Definition* in the section and the applicable ACU manual for detailed information.

- 15 Door Output Relay.** Enter the number of the 422 relay.
- 16 DKR Configuration.** Enter the ID number. Valid ranges of numbers is from 1-9999.
- 17 ABA Configuration.** Enter the ID number Valid range of numbers is from 1-9999.
- 18 Keypad Enable.** A Y / N field to activate the associated keypad.
- 19 Keypad Active During Building Modes.** A Y/N field to indicate whether the keypad should be activated during the building open, limited and / or closed mode.
- 20 Keypad Active During Time Codes.** Up to four time codes

**SE 818 READER REPORT DEFINITION [rdr3entr]**

```

[rd3entr]          SE/818 Reader Report Definition
  1 Reader Mode    : 2
  3 DKR/SCR Fail Rpt : 0
  Coax Failure    : 19
  Forced Open    : 1E
  Access Granted : 1
  Key Trace      : 5
  Exit Granted   : 3
  VIP Failure    : 7
  2 Proximity Type : 0
  Sensor Failure : 22
  Door Open Too Long : 6
  Access Denied  : 4
  Exit Denied   : 4
  MSM Failure    : 7
  VIP Tamper     : 7
  4 DKR Configuration : 0
  5 VIP Enable: N
  6 VIP Active During Building Modes:
  7 VIP Active During Timecodes: 1) 0
                                   2) 0
                                   3) 0
                                   4) 0
  Open   Limited   Closed
  N      N          N

```

**Reader Mode.** Optional. Enter the appropriate reader mode number. 0 = Normal, 1 = Open, 2 = Closed, 3 = Station. Default is 0.

**Proximity Type.** Enter the proximity type: 0 = Sensor interface, 1 = DigiKey reader.

- 3 The following thirteen fields, *DKR/SCR Fail* through *VIP tamper*, require the entry of a report number. The word report in this context identifies a user-defined action or series of actions that the ACU is to take in response to various events occurring within the system. (The field titles indicate the event types.) See *Device Report Definition* in this section and the applicable ACU manual for detailed information.
- 4 **DKR Configuration.** Enter the ID number. Valid range is from 1-9999.
- 5 **VIP Enable.** Optional. A Y/N/O field to enable/disable the VIP (O indicates VIP only). Default is N.
- 6 **VIP Active During Building Modes.** Optional. A Y/N field to activate/deactivate the VIP for building modes Open, Limited and Closed. Default is N for all three.
- 7 **VIP Active During Time Codes.** Optional. Enter up to four time code IDs when the VIP is to be active. Default is 0 for all four.

## SE NEXSENTRY READER REPORT DEFINITION [rdr4entr]

| [rdr4entr] |                                   | SeXSENTRY Reader Report Defaults |    |   |                    |   |         |
|------------|-----------------------------------|----------------------------------|----|---|--------------------|---|---------|
| 1          | Reader Mode                       | :                                | 0  | 2 | Proximity Type     | : | 1       |
| 3          | DKR/SCR Fail                      | :                                | 1  |   | Door Open Too Long | : | 1       |
|            | Forced Open                       | :                                | 1  |   | Access Denied      | : | 1       |
|            | Access Granted                    | :                                | 1  |   | Exit Denied        | : | 1       |
|            | Key Trace                         | :                                | 1  |   | Device Tamper      | : | 1       |
|            | Exit Granted                      | :                                | 1  | 4 | DKR Configuration  | : | 1       |
|            | VIP Failure                       | :                                | 1  |   | RSP Type           | : | 0       |
|            | RSP Failure                       | :                                | 0  |   | DKR Configuration  | : | 0       |
| 5          | VIP Enabled:                      |                                  | N  |   | Open               |   | Open    |
| 6          | VIP Active During Building Modes: |                                  |    |   | Limited            |   | Limited |
| 7          | VIP Active During Timecodes:      |                                  |    |   | Closed             |   | Closed  |
|            |                                   |                                  | 01 |   |                    |   |         |
|            |                                   |                                  | 20 |   |                    |   |         |
|            |                                   |                                  | 30 |   |                    |   |         |
|            |                                   |                                  | 40 |   |                    |   |         |

**Reader Mode.** Optional. Enter the appropriate reader mode number. 0 = Normal, 1 = Open, 2 = Closed, 3 = Station. Default is 0.

**Proximity Type.** Enter the proximity type: 0 = Sensor interface, 1 = DigiKey reader.

- 3 The following eleven fields, DKR/SCR Fail through Device Tamper, require the entry of a report number. The report in this context identifies a user-defined action or series of actions that the ACU is to take in response to various events occurring within the system. (The field titles indicate the event types.) See Device Report Definition in this section and the applicable ACU manual for detailed information.
- 4 **DKR Configuration.** Enter the ID number. Valid range is from 1-9999.
- 5 **VIP Enable.** Optional. A Y/N/O field to enable/disable the VIP (O indicates VIP only). Default is N.
- 6 **VIP Active During Building Modes.** Optional. A Y/N field to activate/deactivate the VIP for building modes Open, Limited and Closed. Default is N for all three.
- 7 **VIP Active During Time Codes.** Optional. Enter up to four time code IDs when the VIP is to be active. Default is 0 for all four.

## POINTS [pnt\_entr]

Enter individual point IDs for all input and output points in the system.

### Note:

There are eight hardware types (exclusively input and/or output contacts) that require a type number and a point number when being set up in the database. You establish these devices using the *Point Entry* screen and cause the log messages to differ depending upon point type:

1. **Alarm.** An input contact for monitoring conditions defined as alarms.
2. **Door Switch.** An input contact for determining the open/closed status of a door (only used when associated with a door record).
3. **REX.** An input contact for determining the status of a request-to-exit switch.
4. **Open On REX.** An input contact for determining the status of a request-to-exit switch which requires an action by the computer to unlock a specific door.
5. Not used.
6. **General.** An input or output contact for general purpose use. This function generates an input active message.
7. **Camera** (optional feature). Input / output contact for camera system monitoring and control.
8. **Spitter** (optional feature). Input contact to indicate a ticket pull for a parking control system.
9. **Guard Tour** (optional feature). An input contact allowing guard tour activity monitoring.

A sample screen follows:

---

```

[ptnt_entr]                Point Entry
1 Point ID: 101            2 Point Description: 422 22 (0.0)
3 Device ID : 100 = DIAL-UP 422 01
  (Computer ID: 100 Poller # : 0 Address: 1 )
4 Sensor/Board: 1        5 Contact: 1
6 Point Type : 6 - General                                7 Time : 15
8 Point Mode : 0        9 Input/Output : I 10 Watchdog: 0 11 000 Report #: 00
12 Enable Point: 0      13 Disable : N
14 Zone Number : 0 = ALL ENCOMPASSING
15 Tenant : 0 = ALL ENCOMPASSING

16 Code Mod Start End Mon Tue Wed Thu Fri Sat Sun Hol
Tim Cd 1: 1 G = 00:00 23:59 Y Y Y Y Y Y Y Y
Tim Cd 2: 0 0 = 00:00 00:00 N N N N N N N N
Tim Cd 3: 0 0 - 00:00 - 00:00 - N N N N N N N N
Tim Cd 4: 0 0 - 00:00 - 00:00 - N N N N N N N N

```

**Point ID.** Required. Enter a four-digit maximum point ID number.

**Point Description.** Optional. Enter a 20-character maximum description of the point. If omitted, the system enters the point ID number into this field.

- 3 **Device ID.** Required (*zoom* available). Enter a four-digit maximum device ID number that is attached to this point. Once entered, the system automatically enters the associated computer number, poller number, and address fields.
- 4 **Sensor/Board.** Required. The sensor number or board number through which this point communicates. A point may be connected through a multiple switch monitor (MSM) to an ACU, or it may be connected directly to other device types. For an ACU, the number entered is the number of the sensor connection to the device. For devices with directly connected points (e.g., Optomux boards, alarm monitoring devices), enter 0 (zero), or the board number if multiple boards are connected on the same poller. Note that for WSE 422, 0 is for input points and 1 is for output points.
- 5 **Contact.** Required. For points connected through an MSM to an ACU, enter the MSM point contact number (1, 2, 3, or 4). For directly connected devices, enter the contact number for that device (0 through 15). Note for WSE 422, 0-75 is for inputs and 0-51 if for outputs. Refer to the WSE 422 input/output tables at the back of this section.
- 6 **Point Type.** Required (*zoom* available). Enter the point type number in the range 1 through 9 as described above, or screen-check using F7 (*zoom*).

- 
- 7 Time.** Required for point type 2 (door switch) and 6 (general, when used with an OPTO 22); disregard for all other types. For type 2, enter the number of seconds before the door is to be considered held open. The range is 1 through 240 (the default is 15 seconds and this is the recommended value for normal usage). For type 6, and if this is an output point, enter the number of seconds that the OPTO 22 output remains active. The range is 0 through 655 (0 indicates no time limit).
- 8 Point Mode.** Required except for MSMs; enter 0 if this the case. Enter 0 (zero) if the point is normally open; enter 1 if the point is normally closed. Default is 0.
- 9 Input/Output.** Required. Enter I for an input point; enter O (letter O) for an output point. Default is I.
- 10 Watchdog.** Required for Opto 22 devices only. Indicates the action to be taken if communication is interrupted between the host computer and the device. Enter:
- 0 — No action (default)
  - 1 — Open on time-out
  - 2 — Close on time-out

**808 Report #.** Required for points attached to 8xx-series ACUs. Note that this is used with alarm generated points. If it is a door switch or a REX, it is defined on the second page of the Reader screen. The word report in this context identifies a previously-defined action that the ACU is to take in response to specific events. Up to 15 reports can be defined for each ACU (see the respective ACU manual for detailed information). Enter a number in the range 1 through 15 indicating the 808 report to be used. If omitted, Report #1 — report to host at all times — is used by default.

- 12 Enable Point.** Conditional (*zoom* available). Indicates a point ID that must be activated before the current point can be activated. Enter the enable point ID number. This is only active for host control points.

#### NOTE

The *Enable Point* is primarily used with closed circuit television monitors (CCTVs), but can be used elsewhere. For example, in order to open a parking lot gate, a car must first be sensed by a detector (enable point). Then when the proper keyholder uses their key, the gate opens, allowing access.

- 13 Disable.** Required. A Y/N field indicating if the point is currently disabled (Y). Default is N (point currently active). Note that an intelligent ACU will only control host action not the physical action at a site where the ACU reports a contact closure.
-

- 14 **Zone number.** Required (*zoom* available). Enter the zone number applicable for this point. The system enters the default value of 0 (zero) if this field does not apply.
- 15 **Tenant.** Required (*zoom* available). Enter the tenant number applicable for this point. The system enters the default value of 0 (zero - system owner) if this field does not apply.
- 16 **Tim Cd (1-4), Code and Mod.**

**Code:** Required (*zoom* available). Four time codes can be entered to allow input monitoring at this point. The default is time code #1.

#### NOTE

The system effectively shunts points and devices not covered by an active time code. Recommend controlling events through reporting when using an intelligent ACU.

**Mod:** Optional. Log messages and system action can be modified using the custom transaction modifier codes A, B, etc., (see *Section 6, System Administration*). Default is 0 and uses standard messages.

## AUTO OPENS / ACTIVATES

The auto open / activate feature is used to instruct the system to lock / unlock doors, or activate / deactivate output points, for a predefined amount of time. Examples:

- A regular business door is configured to automatically unlock at a prescribed time each morning. The time code then re-locks the door at close of business each day.
- Via an output point, a time code automatically switches on an outside light each evening at a prescribed time. The same time code then automatically switches off the light at a prescribed time the following morning.

A sample screen follows:

```

[autoentr]      Auto Open/Activate Entry
1 Serial #: 10426
2 Reader ID
  or Point ID: 1375 - B1B #7 DOOR #7
3
      Start End Mon Tue Wed Thu Fri Sat Sun Hol
Timecode: 16 - 11:59-13:01 Y Y Y V Y M N N

```

**Serial #.** A nine-digit maximum control number automatically generated and displayed by the system when a new auto open / activate code is added. This information is not entered by the user.

**Reader ID or Point ID.** Required. Enter the applicable reader or output point ID number.

**3 Timecode.** Required. Enter the applicable time code.

## DEVICE REPORT DEFINITION [rdefentr]

Use this feature to create action reports for the SE 8xx-series and SE 422 ACUs. An action report is a set of user-defined tasks performed by the ACU when specified conditions occur. The actions are defined using the device report definition screen (sample screen shown below); the reports are assigned using screens described in the device entry subsection. For complete descriptions on how to use the report definition screen for the various ACU types, please refer to the respective ACU manuals.

### NOTE

The list of time conditions in the left hand side of the screen (Time Code A-C) and the task choices running left to right, such as Send To Host are used to define actions. To define an action, type a Y or N, or a number as appropriate for the desired task in the field under the appropriate task choice. For example, if you want the report to send information to the host when the building is in the open mode, type Y in the Bldg Open field under the Send to Host column.

| [rdefentr] Report Definition Entry |              |                      |              |
|------------------------------------|--------------|----------------------|--------------|
| Device ID                          | 2883         | = ALPHA LAB BBSX #10 | Report # 4   |
|                                    | Send To Host | Close Latch          | Close Output |
| Bldg Open                          | Y            | N                    | N            |
| Bldg Limited                       | N            | N                    | N            |
| Bldg Closed                        | N            | N                    | N            |
| Time Code A                        | 1            | 0                    | 1            |
| Time Code B                        | 0            | 0                    | 0            |
| Time Code C                        | 0            | 0                    | 0            |
| Contact Num                        |              |                      | 4            |
| Print Asterisk With Log            | N            | Prevent Bldg Closure | N            |

## SE 422 PIN DEFINITION

The number of PIN digits and the PIN seed must be defined and entered. The seed is used as part of an equation to calculate PIN numbers assigned to keyholders.

Assigned PIN numbers can be printed out (see *Section 3, SE 422 PIN Master Report*). Also, it is possible, but not recommended, to override the system-wide default values entered here (see *Device Entry, SE 422*, in this section). A sample data entry screen follows:

```
[pnd]entr]      SE 422 PIN Entry
  ① PIN Digits: 4      ② PIN Seed: 10000
```

**PIN Digits.** Optional. Enter 4 or 5. Default is 4.

**PIN Seed.** Optional. Enter a number in the range 0 — 999999. Default is 0.

## SE 422 HARDWARE DEFINITION

Various special-function subdevices may be connected to the SE 422. These include input monitoring or output control devices (MIROs), proximity key or magnetic stripe card readers, and keypads allowing PIN entry.

The subdevices as connected to the SE 422 are known as nodes on the SE 422 communications network. A node is further defined by assigning it a point ID, by entering the device ID of the SE 422 to which the subdevice is attached, the communication address (node) number of the attachment, the report number to use if the device fails, and the serial number of the subdevice. A sample data entry screen follows.

```
[node]entr]      SE422 Hardware Definition
  ① Point ID      : 5555 = X-SPECIAL SWIPE READER
  ② Device ID    : 4222 = 422 #5 ALPHA LAB
  ③ Node Number  : 18
  ④ Dev Failure Rpt: 2
  ⑤ Serial Number : 3000000000000000
```

**Point ID.** Required. Enter a four-digit point ID and device description.

**Device ID.** Required (*zoom* available). Enter an existing SE 422 device ID.

**③ Node Number.** Required. Note that each node device must have an address (or serial number) assigned to it with the Serial Command during database setup. Enter a node number in the range 1 — 18.

- 4 **Dev Failure Rpt.** Optional. Enter a device failure report number in the range 1 — 32. Default is 0 — No report.
- 5 **Serial Number.** Required. Enter the device serial number (imprinted on a rotary switch).

## DIALER ENTRY

An optional, factory-set remote dial-up poller must be established to enable the remote dial-up feature for 8xx-series ACUs connect to an RDI unit or to a dial-up 422. The dialer entry screen is used to enter various control parameters for the off-site ACUs. A sample screen follows:

```

1 (dialer) Remote Device Entry
2 Device ID : 000 = RDI - ALPHA LAE
3 Associated Poller Id: 3 = RDI/SCHED POLLER #1
4
5 Phone Number Login String Password
6 Remote: .4921342 *****
7 Host1: .9708964 rdi new123
8 Host2: *****
9 Host3: *****
10 No Activity Disconnect Seconds: 90
11 RLC/RDI should: Call when alarm occurs: Y Dial back: N
12 Number of Transactions to hold: 4000
13 Host Retry Minimum Call Max Call
Minutes before: 2 300 720
Schedule Next Call on 03/21/95 at 08:02
Statistics for last successful call: 07/10/95 10:19 F 0
Number of failed call attempts since last success: 0

```

**Device ID.** Required (*zoom* available). Enter a four-digit device ID number (system automatically displays device description).

**Associated Poller ID.** Required (*zoom* available). Enter the remote dial-up (scheduler poller) poller ID number assigned to this device (system automatically displays poller description).

- 3 **Remote.** Required. Enter remote location phone number. Note that if the host must dial a prefix, be sure to include it.
- 4 **Host1.** Required. Enter host phone number. For RDI units only, enter log in string and password (default shown). Note that if the remote must dial an area code or other prefix, be sure to include it.

- 
- 5 **Host2.** Required, if applicable. Enter alternate host #2 phone number. For RDI units only, enter login string and password.
  - 6 **Host3.** Required, if applicable. Enter alternate host #3 phone number. For RDI units only, enter login string and password.
  - 7 **No Activity Disconnect Seconds.** Optional. Enter the number of no activity seconds to elapse before host disconnects from the remote ACU. Default is 90 seconds.
  - 8 **RLC/RDI should:** Two related Y / N fields:
    - **Call when alarm occurs:** Y or N
    - **Dial back:** Y or N — *Not currently implemented.*
  - 9 **Number of transactions to hold:** Optional. Enter the number of transactions to be held in remote memory. Default is 4000.
  - 10 **Minutes before:** Three related fields:
    - **Host Retry.** Number of minutes to wait before retrying call to host for example, every two minutes.
    - **Minimum Call.** Minimum elapsed time before dialing remote site for log messages (in hours) for example, every six hours.
    - **Max Call.** Maximum elapsed time before dialing remote site for log messages (in hours) for example, every 12 hours.
- Schedule Next Call on / at.** Enter the time and date when next call is to be made. Note that a future date will cause the scheduler to Not dial the devices until the future date/tune is reached.
- 12 **Statistics for last successful call** (automatically displayed and updated): **Date, Time, Type, Count.**
  - 13 **Number of failed call attempts since last success** (automatically displayed and updated).

## SITE ENTRY DEFINITION

Site codes restrict the use of one or more doors to specific groups of cards (a particular company, a particular department, etc.). Up to 64 site codes can be assigned to the same card group ID. The group ID is used by ACUs which support ABA magnetic card readers to make access decisions based on site codes. A sample screen follows:

---

```

[altcentr] Site Entry Definition
      ① Group Id ② Code
          100      1000
          101      1001
          6016     7279
          8787     123x
          8787     5678
          9999     0000
          9999     1010
          9999     1X23
          9999     7890
          9999     9898
  
```

- ① **Group ID.** Enter a four-character maximum group ID number.
- ② **Code.** Enter a four-character maximum site code. Enter x in any position to act as a wild card; all characters in that position are matched. With the first 'x entry' in the sample screen, for example, the range 1230 through 1239 would be matched.

## ABA CONFIGURATION ENTRY

The ABA (American Banking Association) configuration entry screen is used to define codes to be read from a standard ABA magnetic stripe card reader, and to define actions to be taken in response to the cards read. A sample screen follows:

```

[abacentr] ABA Configuration Entry
  ① Configuration Id: 1000
  ② Key A:           Start Length
  ③ Key B:           4     2
  ④ Key C:           10    3
  ⑤ Expiration Date Start: 19 ⑥ Site Code Start: 20
  ⑦ ABA Card Data Action : 0
  ⑧ Based on key number : N      Deny Access During Fail Soft
  ⑨ Based on site code  : N      Deny Access
  ⑩ Based on expiration date: N   Deny Access
  ⑪ Use site code as key : N      Deny Access
  
```

- ① **Configuration ID.** Enter a four-character configuration ID number.
- ② **Key A.** Start position and length of first part of key. Key fields A, B and C are linked to form the key field.

- ③ **Key B.** Start position and length of second part of key.
- ④ **Key C.** Start position and length of third part of key.
- ⑤ **Expiration Date Start.** Expiration date start position.
- ⑥ **Site Code.** Site code start position.
- ⑦ **ABA Card Data Action.** The report number (ID) that will execute in response to an ABA card swipe event.
- ⑧ **Based on Key Number.** Y / N — Actions to take that are based on the key number.
- ⑨ **Based on Site Code.** Y / N — Actions to take that are based on the site code.
- ⑩ **Based on Expiration Date.** Y / N — Actions to take that are based on the expiration date.
- ⑪ **Use Site Code as Key.** Y / N — Use the site code as the key number.

## DKR CONFIGURATION ENTRY

The DKR (Digital Key Reader) configuration entry screen is used to change the factory-set operational default values. A brief introduction to these procedures is given here, but for complete information consult the appropriate DKR manual. *In all cases, however, do not attempt these procedures without first contacting your dealer and/or WSE customer support.*

```

[dkrcntrl]    DKR Configuration Entry
① Configuration Id: 1
② Send Key To ACU Once: Y
③ Read Range: 255 ④ Number Of Reads: 2 ⑤ Read Time: 210
⑥ LED and Beeper Setup
      On Time  Off Time  Duration
Beeper   : 32      32      64
Red LED  : 0       0       0
Green LED: 0       0       0
  
```

**Configuration ID.** Enter a configuration ID number in the range 1 — 9999.

**Send Key to ACU Once.** Controls the number of times the key number is forwarded to the ACU while within the read-range of the reader. The default is Y—Once.

- 3 **Read Range.** Controls the maximum read range available with the particular digital reader. The range is 0—255; default is 255.
- 4 **Number of Reads.** Controls the number of additional verification reads of a single key within the sensor's range before declaring the key valid. The range is 0—255; default is 1.
- 5 **Read Time.** Controls the amount of time that the reader retains the key number in memory after the key is removed from the sensor's read range. The valid range is 0—65535 clock ticks (100 clock ticks is equal to 1 second); default is 100.
- 6 **LED and Beeper Setup.** Beeper, Red LED, and Green LED on-time, off-time, and duration. Override the default operation of the beeper, Red LED, and Green LED on the digital key reader in response to a valid key read. The valid range for on-time, off-time, and duration is 0-65535 clock ticks. The default is 0 (uses factory-set predefined behavior).

## USER-DEFINED INFORMATION

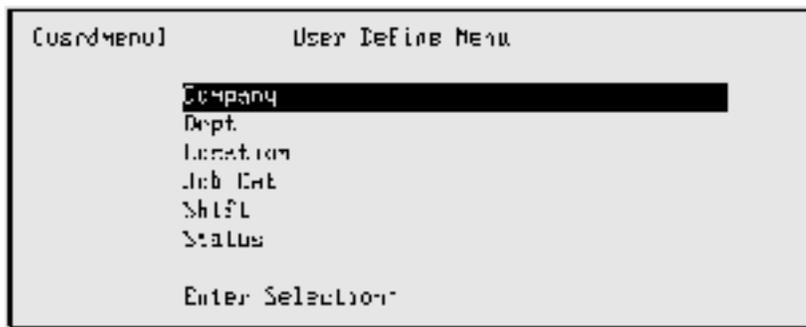
Certain field titles on the keyholder record screens can be changed to suit the individual SE 6000 owner. Since keyholder records may be considered the primary data items for an access control system, many SE 6000 owners use the field title change feature to tailor the system to their precise requirements (these fields are provided for informational purposes and for use as report selection criteria, and have no effect on system processing).

The field titles are changed with the control file maintenance feature accessed from the System Administration menu (see *Section 6: System Administration*):

```
[ctrlent] Control File Maintenance
Company Name Security Electronics
Field titles: Enter "unused" for fields not required
Fields on Page 1 of the Keyholder Entry screen:
A: Company      B: Dept         C: Location
D: Job Cat      E: Shift       F: Status

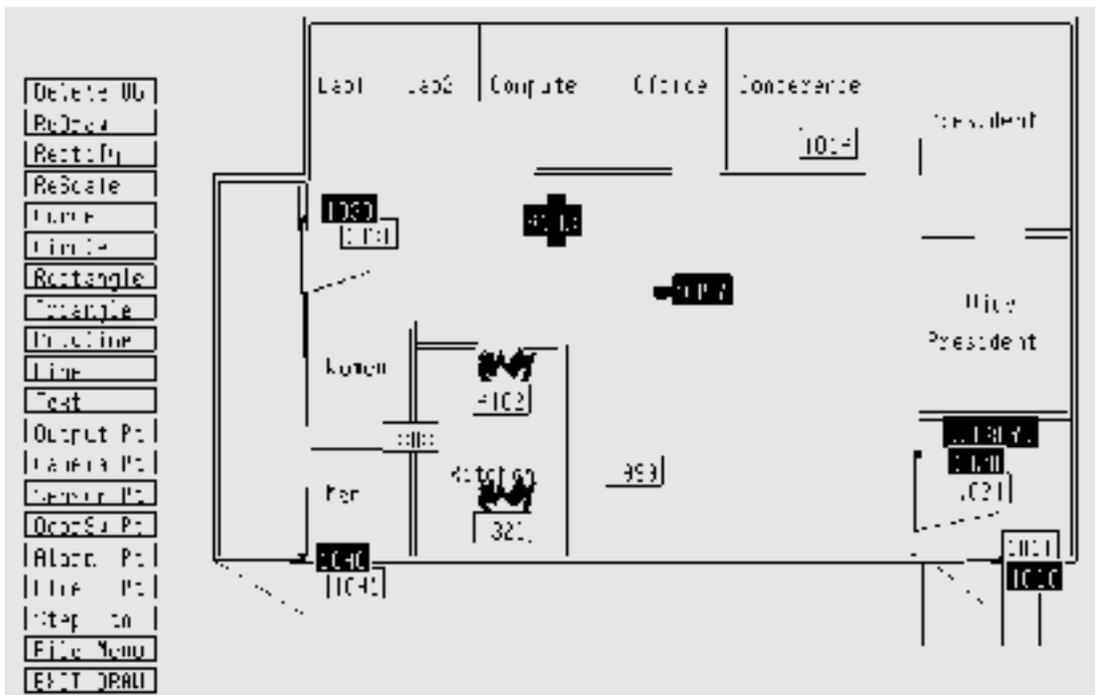
Fields on Page 2 of the Keyholder Entry screen:
1: usr1         2: usr2         3: usr3
4: usr4         5: usr5         6: usr6
7: Remarks
```

The user-defined information selection here in the master file entry menu is used to assign descriptions to these fields. A sample screen follows: Note that a description of "unused" will skip the field during keyholder file maintenance.



## MAPS

The DRAWMAPS function is used by the event monitoring function to display the location of doors, points, alarms, etc. To use this feature on an SE 6200 and above, it must be operating under the Reflection 4 terminal emulation software (mouse required). You can also use this feature on an SE 6100 or below from your console. This requirement is due to the SCO Unix graphic memory limitation. The function has several built-in HELP maps, and drawing instructions display at the foot of all screens. A sample map follows:



## MAP DRAWING COMMANDS AND DESCRIPTIONS

| COMMAND   | DESCRIPTION   |
|-----------|---|
| Delete Ob | Remove graphics and text. Once selected, the menu list shows only those object types currently on the map. Select one, then follow deletion instructions. |

---

|                  |  |
|------------------|--|
| <b>ReDraw</b>    | Redraws screen. Use if graphics appear incorrect.  |
| <b>Rectify</b>   | Makes all lines <i>close</i> to horizontal or vertical <i>exactly</i> horizontal or vertical. Lines <i>nearly</i> 45° are drawn at <i>exactly</i> 45°. |
| <b>Rescale</b>   | Rescale (resize) map. Lines and curves change; text and icons do not change.   |
| <b>Curve</b>     | Draw curved lines.   |
| <b>Circle</b>    | Draw circles.  |
| <b>Rectangle</b> | Draw boxes.  |
| <b>Triangle</b>  | Draw triangles.  |
| <b>Polyline</b>  | Draw connected lines.  |
| <b>Line</b>      | Draws a single line.   |
| <b>Text</b>      | Create text labels (large and small).  |
| <b>Outpt Pt</b>  | Output point icon — Rectangle with a smaller rectangle crossing it (point 4103 on sample map).   |
| <b>Camera Pt</b> | Camera point icon — Rectangle with a small projection to the left (point 9997 on sample map).  |
| <b>Sensor Pt</b> | Sensor point icon — Black rectangle when locked; white when unlocked (point 1030 on sample map).   |
| <b>DoorSw Pt</b> | Door switch icon (point 1031 on sample map).   |
| <b>Alarm Pt</b>  | Alarm point icon — Red rectangle (point 999 on sample map).  |
| <b>Fire Pt</b>   | Fire point icon. The icon shows a red and yellow flame above a rectangle (point 4102 on sample map).   |
| <b>File Menu</b> | Switch to File Menu to load, save, rename, copy, delete, or start new maps.  |
| <b>EXIT DRAW</b> | Exit DRAWMAPS program.   |

---

**SE 422 Input Table**

|                 |     | 0  | 1  | 2  | 3  | 4  | 5  | 6  |
|-----------------|-----|----|----|----|----|----|----|----|
| ACU (2-state)   | 0:  | 1  | 2  | 3  | 4  | 5  | 6  | 7  |
| M16 /RO1        | 1:  | 8  | 9  | 10 | 11 | 12 | 13 | 14 |
| (4-state input) | 2:  | 15 | 16 | 17 | 18 | 19 | 20 | 21 |
|                 | 3:  | 22 | 23 | 24 | 25 | 26 | 27 | 28 |
|                 | 4:  | 29 | 30 | 31 | 32 | 33 | 34 | 35 |
|                 | 5:  | 36 | 37 | 38 | 39 | 40 | 41 | 42 |
|                 | 6:  | 43 | 44 | 45 | 46 | 47 | 48 | 49 |
|                 | 7:  | 50 | 51 | 52 | 53 | 54 | 55 | 56 |
|                 | 8:  | 57 | 58 | 59 | 60 | 61 | 62 | 63 |
| RO4 (4-state)   | 9:  | 64 |    |    |    |    |    |    |
|                 | 10: | 65 |    |    |    |    |    |    |
|                 | 11: | 66 |    |    |    |    |    |    |
|                 | 12: | 67 |    |    |    |    |    |    |
| VIP (2-state)   | 13: | 68 |    |    |    |    |    |    |
|                 | 14: | 69 |    |    |    |    |    |    |
| SI (4-state)    | 15: | 70 | 71 |    |    |    |    |    |
|                 | 16: | 72 | 73 |    |    |    |    |    |
| MSR (2-state)   | 17: | 74 |    |    |    |    |    |    |
|                 | 18: | 75 |    |    |    |    |    |    |

|   |
|---|
| Input points are always on sensor 1, contact 1-75 |
|---|

**SE 422 Output Table**

|                 |     | 0  | 1  | 2  | 3  | 4  | 5 |
|-----------------|-----|----|----|----|----|----|---|
| Acu (2-state)   | 0:  |    | 1  | 2  | 3  | 4  | 5 |
| M16/RO1         | 1:  | 6  | 7  |    |    |    |   |
| (4-state input) | 2:  | 8  | 9  |    |    |    |   |
|                 | 3:  | 10 | 11 |    |    |    |   |
|                 | 4:  | 12 | 13 |    |    |    |   |
|                 | 5:  | 14 | 15 |    |    |    |   |
|                 | 6:  | 16 | 17 |    |    |    |   |
|                 | 7:  | 18 | 19 |    |    |    |   |
|                 | 8:  | 20 | 21 |    |    |    |   |
| RO4             | 9:  | 22 | 23 | 24 | 25 | 26 |   |
|                 | 10: | 27 | 28 | 29 | 30 | 31 |   |
|                 | 11: | 32 | 33 | 34 | 35 | 36 |   |
|                 | 12: | 37 | 38 | 39 | 40 | 41 |   |
| VIP             | 13: |    | 42 | 43 | 44 |    |   |
|                 | 14: |    | 45 | 46 | 47 |    |   |
| SI              | 15: |    |    |    |    |    |   |
|                 | 16: |    |    |    |    |    |   |
| MSR             | 17: |    | 48 | 49 |    |    |   |
|                 | 18: |    | 50 | 51 |    |    |   |

|  |
|--|
| Output points are always on sensor 2, contact 1-51 |
|--|

# SECTION 5

# MASTER FILE REPORTS

## INTRODUCTION

The master file reports list comprehensive database information. The report menu screens are accessed via the master file reports menu [rprtmenu], displayed via the main menu. In this section, the reports are documented following the reports menu sequence (see section table of contents). A sample [rprtmenu] screen follows:

```
replace stored | update | record 1 of 14 records found
[rprtmenu]      Master File Reports
  Keys Master
  Access Assignments
  Access Definition
  Time Codes
  Holidays
  Tenants
  Company
  Dept
  Location
  Job Cat
  Instructions
  Maps
  Device Configuration Reports
  SE/422 PIN Report
  Enter Selection:
  Pro Fcch | Next Fcch | 4 | 5:31 | Mode | Store | 7 | 8
```

All screens in this section show the system default values, with most screen fields requiring a numeric range entry. For example, the default range for keyholders is 1 — 999999999 (to reduce waiting time while a report is generating, enter the smallest range of numbers for each category which will still provide the information wanted). Other screen fields include choices for date ranges, regular or extended information, and report sequencing. When all fields have been entered, press Enter (Yes - default) to begin report generation:

```
Ready to produce Report. OKay to continue?(yes/no)(yes)
1 2 3 4 5 6 7 8
```

Once compiled, a report output selection displays. Normally, 1 (system report printer) or D (display at terminal) is chosen. The system also gives the option to print to a terminal printer. Report totals are printed at the end of each report.

## ADDITIONAL INFORMATION

An additional report feature not accessed via the reports menu, *132-xx Column Report Display*, is detailed at the end of this section.

## KEYS MASTER

Two versions of the keyholder master report are available — Keyholder Quick List and Keyholder Master List (extended). The quick report includes keyholder ID, key number, keyholder name, information from user-defined fields B and D, phone number, title, user-defined field C, and floor. The master report includes all the keyholder information entered on page 1 of the keyholder entry screen, plus address, phone number, and user-defined field 7. Also, the master report prints access code information (first 20 codes) for each keyholder. A sample [key\_rprt] screen follows:

Note that certain report screens include a sort sequence field and a numbered list of sort sequence categories. Enter one of the numbers into this field to print data related to that sequence number. For example in the Keyholder Master Report screen, enter number 1 in the Sort Sequence field to sort data by keyholder ID (see the following example).

```

[key_rprt]      Keyholder Master Report
                Lower Limit Upper Limit
Keyholder ID   : 0          999999999
Company        : 0          99
Dept           : 0          9999
Location       : 0          9999
Job Cat        : 0          99999
Issue Date     : *****  11/08/95
Key Number     : 0          99999999
Shift          : ****      zzzz
Status         : ****      zzzz
Tenant         : 0
Extended Info ? : N
Sort Sequence:  1      1> Keyholder ID
                  2> Company, Name
                  3> Dept, Name
                  4> Location, Name
                  5> Issue Date, Name
                  6> Name, Keyholder ID

```

## KEYHOLDER QUICK LIST — SAMPLE REPORT

| 06/02/96<br>14:45 |            | BAYOU INDUSTRIES<br>Key Quick List |       |      |          | Page 1                |      |
|-------------------|------------|------------------------------------|-------|------|----------|-----------------------|------|
| Keyholder         | Key No     | Keyholder Name                     | Dept. | Pos. | Phone    | Title                 | Bldg |
|                   | 220774 409 | JENSEN STEVE                       | 11    | 6    |          |                       | 18   |
|                   | 221922 811 | KREBS SCOTT                        | 11    | 6    |          |                       | 18   |
|                   | 222172 512 | DUNN JEFF                          | 11    | 7    | 123-4567 |                       | 18   |
|                   | 233132 588 | NEWMAN TERESA                      | 11    | 0    | 890-1234 | RECEPTIONIST          | 18   |
|                   | 239445 277 | CLEMENT KAREN                      | 11    | 0    |          |                       | 5    |
|                   | 245165 338 | KIRK KATHY                         | 11    | 6    |          | PINKERTON SECURITY    | 18   |
|                   | 246763 445 | FERRELL STUART                     | 11    | 7    | 567-8901 | SECURITY MGR          | 18   |
|                   | 247666 176 | KERR KATIE                         | 11    | 0    |          |                       | 0    |
|                   | 248112 765 | LOWE LORRAINE                      | 11    | 7    | 234-5678 | SECURITY RECEPTIONIST | 2    |
|                   | 249343 453 | GREENWOOD LORI                     | 11    | 7    | 901-2345 | SECURITY RECEPTIONIST | 1    |

## KEYHOLDER HOLDER MASTER REPORT — SAMPLE REPORT

08/02/96  
PAGE 1  
10:58  
McArthur Complex  
Keyholder Master List

|              |                                       |           |                   |          |               |
|--------------|---------------------------------------|-----------|-------------------|----------|---------------|
| Keyholder    | 222541                                | Name      | Cross, Gregory    | Company  | 2 = J o h n s |
| Lynne        |                                       | Company   |                   |          |               |
| Key No       | 2332                                  | Addr1     | 1917 Blair Avenue | Dept     | 2 =           |
| Engineering  |                                       |           |                   |          |               |
| S.S. No      | 123-45-6789                           | Addr2     | Weston, CA 95199  | Location | 5 = S a n t a |
| Clara Annex  |                                       |           |                   |          |               |
| Tenant       | 1                                     | Addr3     |                   | Job Cat  | 14 = Software |
| Engineer     |                                       |           |                   |          |               |
| P.I.N.       | 1314                                  | Privledge | YES               | Shift    | 0 = N/A       |
| Remarks      | Occasional late evening, weekend work |           |                   | Status   | 0 = N/A       |
| Phone        | (123)456-7890                         | Trace N   | Visitor YES       | Issued   | 07/14/96      |
| Returned     | *****                                 |           |                   |          |               |
| Access Codes | 1 4 7 8 21                            |           |                   |          |               |

## ACCESS ASSIGNMENTS

### KEYHOLDER ACCESS ASSIGNMENT

This report prints the access codes and access groups assigned to keyholders. Regular and extended versions of the report are available.

The regular report lists keyholder numbers and names, access code / group numbers and descriptions, and access override codes where applicable. The extended report includes this data and also gives key number, social security number, tenant number, PIN, company, department, location, job category, shift, status, remarks, phone, trace, visitor, and badge issue information. A sample screen follows:

```

[egprprt] Keyholder Access Assignment Report

Keyholder ID   :  B      Lower Limit  Upper Limit
Access Group   :  B      999999999
Access Code    :  B      9999
Override Code  :  B      9999
Tenant Number  :  B
Extended Info  :  N

Sort Sequence  :  1  1) Name, Access Code, Access Group
                   2) Emp. ID, Access Code, Access Group
                   3) Access Code, Name, Access Group
                   4) Access Group, Name, Access Code
                   5) Company      , Access Code, Name
  
```

### KEYHOLDER ACCESS ASSIGNMENT: REGULAR — SAMPLE REPORT

| Keyholder | Keyholder Name    | Code | Code Description   | Group | Group Description | Override |
|-----------|-------------------|------|--------------------|-------|-------------------|----------|
| 23342     | Smith, James      | 1    | Host 422, 708, 818 | 1     | Main              | 0        |
| 22243     | Stevens, Sandy    | 1    | Host 422, 708, 818 | 1     | Main              | 0        |
| 21188     | Svensen, Lars     | 1    | Host 422, 708, 818 | 1     | Main              | 0        |
| 23397     | Swenson, Lawrence | 1    | Host 422, 708, 818 | 1     | Main              | 0        |
| 24411     | Tauber, Linda     | 1    | Host 422, 708, 818 | 1     | Main              | 0        |



## ACCESS DEFINITION

### ACCESS CODE MASTER

This report details all access codes defined in the system (the report can be limited to a single code or a range of codes, as required). A sample screen follows:

```

[4/20/96] Access Code Master Report

          Lower Limit   Upper Limit
Access Code ID :      1           9999
Reader ID      :      0           9999
Tenant        :      0

Print Elevator Information : N
Sort Sequence : 1  1) Access Code ID
                2) Reader ID
  
```

### ACCESS CODE MASTER LIST — SAMPLE REPORT

| 05/02/96 |                  | Soames Industries       |                    |      |       |       |     | Page 1 |     |     |     |     |     |     |
|----------|------------------|-------------------------|--------------------|------|-------|-------|-----|--------|-----|-----|-----|-----|-----|-----|
| 11:26    |                  | Access Code Master List |                    |      |       |       |     |        |     |     |     |     |     |     |
| Code     | Code Description | Reader                  | Reader Description | Tmcd | Start | End   | Mon | Tue    | Wed | Thu | Fri | Sat | Sun | Hol |
| 12       | Weekend Rcvng    | 22                      | Receiving #1       | 14   | 09:00 | 15:00 | N   | N      | N   | N   | N   | Y   | Y   | N   |
| 13       | Holiday Rcvng    | 22                      | Receiving #1       | 15   | 09:00 | 12:00 | N   | N      | N   | N   | N   | N   | N   | Y   |
| 19       | Lab After Hrs    | 06                      | Lab Main           | 05   | 15:30 | 23:59 | Y   | Y      | Y   | Y   | Y   | N   | N   | N   |
| 20       | Lab Weekends     | 06                      | Lab Main           | 06   | 09:00 | 23:59 | N   | N      | N   | N   | N   | Y   | Y   | Y   |

### ACCESS GROUP MASTER

This report details all access groups defined in the system (the report can be limited to a single group or a range of groups, as required). A sample screen follows:

```

[4/20/96] Access Group Master Report

          Lower Limit   Upper Limit
Access Group ID :      1           9999
Access Code    :      0           9999
Tenant        :      0

Sort Sequence: 1  1) Access Group ID
                2) Access Code ID
  
```

**ACCESS GROUP MASTER LIST — SAMPLE REPORT**

| Group             | Group Description                                | Code | Code Description            | SFS |
|-------------------|--|------|-----------------------------|-----|
| 06/10/96<br>10:03 | HIGHLAND ELECTRONICS<br>Access Group Master List |      | Page 1                      |     |
| 1                 | DWNLD 801/802/8100/4222                          | 5    | DWNLD 801 ACCESS CODE       | N   |
| 1                 | DWNLD 801/802/8100/4222                          | 6    | DWNLD 802 ACCESS CODE       | N   |
| 2                 | SFS/708/801/802/8100/4222                        | 1    | HOST 422, 808 & 708         | N   |
| 2                 | SFS/708/801/802/8100/4222                        | 3    | DWNLD 804 ALPHA LAB 808S #2 | N   |
| 2                 | SFS/708/801/802/8100/4222                        | 4    | DWNLD 805 ALPHA LAB 808S #3 | N   |

**ACCESS OVERRIDE**

The report lists access override codes in the database, with descriptions, start / end dates, and permissions (allow / deny access). A sample screen follows:

```
[acourprt] Access Override Report

Ready to produce Report. Okay to continue? (Y/N) [Y]
```

**ACCESS OVERRIDE — SAMPLE REPORT**

| Code              | Description                                   | Start    | End      | Permission |
|-------------------|---|----------|----------|------------|
| 03/25/96<br>08:21 | Security Electronics<br>Access Override Codes |          | Page 1   |            |
| 1                 | TEST OVERRIDE ALLOW                           | 03/21/96 | 03/24/96 | Allowed    |
| 2                 | TOXIC CHEMICALS IN USE                        | 04/14/96 | 04/14/96 | Allowed    |
| 900               | RDI OVERRIDE CODE                             | 05/11/96 | 05/11/96 | Denied     |
| 999               | TEST OVERRIDE DENIED                          | 05/25/96 | 05/26/96 | Denied     |

**INTELLIGENT FAIL SOFT REPORT**

The intelligent fail soft report function, used in the event of a communications failure, lists keyholder access permissions for each 708P in the system. The report begins a new page for each device, and shows the readers attached to a device, and the keyholders and their access permissions by individual reader. Fail soft access is used only when a 708P cannot communicate with the host computer. A sample screen follows:

```

[fs_rpt]      Fail Safe Report

              Lower Limit  Upper Limit
Device ID    : 0          9999
Keyholder ID : 0          99999999
Tenant Number: 0

```

### INTELLIGENT FAIL SOFT — SAMPLE REPORT

```

03/25/96                      Soames Industries                      Page 1
08:24                          Intelligent Fail Soft Report

Keyholder  Keyholder Name          7110  7120  7130  7140  7150  7160  7170  7180
-----
67100     708P PARKING CNTR
63455     DIGI FI-GI                Y     Y     Y     Y     Y     Y     Y     Y
61096     GUARD NEW                    Y     Y     Y     Y     Y     Y     Y     Y
61099     1030 ALT+D+P                Y     Y     Y     Y     Y     Y     Y     Y

```

### PROJECT REPORT

The Project Report includes number, description, start / stop times and dates, and current status.

#### NOTE

This report gives project status based on start / stop dates defined by the project entry function compared to the current system date and time. Since the selection criteria and reported status do not consider operator overrides, actual and reported project status may differ.

A sample project report screen follows:

```

[prj_rpt]      Project Report

              Lower Limit  Upper Limit
Project ID    : 0          9999

[include      : 1  1) All projects
                2) Active projects
                3) Inactive projects

Sort Sequence : 1  1) Project ID
                2) Project Active Status

```

## PROJECT REPORT — SAMPLE REPORT

| 03/25/96<br>08:29 |                             | Security Electronics<br>Project Report |        |          |        | Page 1   |
|-------------------|-----------------------------|--|--------|----------|--------|----------|
| Project           | Project Description         | S.Date                                 | S.Time | E.Date   | E.Time | Schedule |
| 1                 | TEST PROJECT #1             | 06/01/96                               | 15:52  | 06/01/96 | 15:56  | Active   |
| 2                 | TEST PROJECT #2             | 06/05/96                               | 07:30  | 06/06/96 | 23:59  | Inactive |
| 5                 | EMERGENCY CIRCUITBOARD REV. | 12/17/96                               | 00:00  | 01/01/99 | 23:59  | Active   |
| 50                | NEW TEST PROJECT            | 06/23/96                               | 00:00  | 06/25/96 | 23:59  | Inactive |
| 51                | LAUNCH                      | 02/16/96                               | 08:00  | 02/20/96 | 17:00  | Inactive |
| 100               | TEST PROJECT #3             | 06/05/96                               | 00:00  | 06/10/96 | 23:59  | Inactive |

## KEYHOLDER PROJECT REPORT

The Keyholder Project Report includes keyholder ID, name, project ID and description, and current status. A sample keyholder project report screen follows:

**NOTE**

This report gives keyholder project status based on start / stop dates defined by the project entry function compared to the current system date and time. Since the selection criteria and reported status do not consider operator overrides, actual and reported project status may differ.

| [ep] rpt]       |             | Keyholder / Project Report                                    |  |
|-----------------|-------------|---|--|
|                 | Lower Limit | Upper Limit   |  |
| Keyholder ID :  | 0           | 99999999  |  |
| Project ID :    | 0           | 9999  |  |
| Include :       | 1           | 1) All projects<br>2) Active projects<br>3) Inactive projects |  |
| Sort Sequence : | 1           | 1) Keyholder ID<br>2) Project ID<br>3) Keyholder Name         |  |

## KEYHOLDER PROJECT REPORT — SAMPLE REPORT

| 05/05/96<br>13:47 |                | Security Electronics<br>Keyholder / Project Report |                     | Page 1   |
|-------------------|----------------|--|---------------------|----------|
| Keyholder         | Keyholder Name | Project  | Project Description | Schedule |
| 661091            | BOB SMITH      | 2  | TEST PROJECT #2     | Active   |
| 661093            | JOHN MILLAR    | 1  | TEST PROJECT #1     | Inactive |

## READER PROJECT REPORT

The Reader Project Report lists project number, description, readers assigned, current status.

### NOTE

This report gives reader project status based on start / stop dates defined by the project entry function compared to the current system date and time. Since the selection criteria and reported status do not consider operator overrides, actual and reported project status may differ.

A sample reader project report screen follows:

```
[prj rpt]      Project /Reader Report
              Lower Limit  Upper Limit
Project ID    : 0          9999
Reader ID     : 0          9999

Include       : 1 1) All projects
              2) Active projects
              3) Inactive projects

Sort Sequence : 1 1) Project ID
              2) Reader ID
```

### READER PROJECT REPORT — SAMPLE REPORT

| 05/05/96<br>13:42 |                                   | Security Electronics<br>Project / Reader Report |              | Page 1                               |
|-------------------|-----------------------------------|---|--------------|--------------------------------------|
| Project           | Project Description               | Schedule  | Reader       | Reader Description                   |
| 10                | TEST PROJECT #1                   | Active  | 8110<br>8120 | 808SX DOOR 1<br>808SX DOOR 2         |
| 15                | EMERG. CIRCUIT BOARD REV. PROJECT | Active  | 1001<br>1010 | 422 ENTRY #1<br>818 #7 DOOR #1 ALPHA |

## TIME CODES

This report lists all time codes set up in the database. A sample screen follows:

```
[tncdprpt]    Time Code Master Report
              Lower Limit  Upper Limit
Time Code:    0          99
```

## TIME CODES — SAMPLE REPORT

| 03/25/96<br>08:36 |                          | Security Electronics<br>Timecode Report |       |     |     | Page 1 |     |     |     |     |     |
|-------------------|--------------------------|---|-------|-----|-----|--------|-----|-----|-----|-----|-----|
| Tmcd              | Description              | Start                                   | End   | Mon | Tue | Wed    | Thu | Fri | Sat | Sun | Hol |
| 0                 | NEVER ACTIVE             | 00:00                                   | 00:00 | N   | N   | N      | N   | N   | N   | N   | N   |
| 1                 | 7-DAYS, 24-HOURS & HOLS  | 00:00                                   | 23:59 | Y   | Y   | Y      | Y   | Y   | Y   | Y   | Y   |
| 2                 | OFFICE HOURS 7 am - 6 pm | 07:00                                   | 18:00 | Y   | Y   | Y      | Y   | Y   | N   | N   | N   |
| 3                 | WEEKENDS & HOLIDAYS      | 00:00                                   | 23:59 | N   | N   | N      | N   | N   | Y   | Y   | Y   |

## HOLIDAYS

This report lists all holidays that have been entered into the system. A sample screen follows:

```
[
      Holiday Master Report

Ready to produce Report. Okay to continue? (Y/N)[Y] █
```

## HOLIDAY CODES — SAMPLE REPORT

| 03/25/96<br>08:38 |                        | Jamestown Aircraft<br>Holiday Master Report |  | Page 1 |  |
|-------------------|------------------------|---|--|--------|--|
| Date              | Description            |   |  |        |  |
| 01/01/96          | NEW YEAR'S DAY         |   |  |        |  |
| 05/27/96          | MEMORIAL DAY           |   |  |        |  |
| 07/04/96          | INDEPENDENCE DAY       |   |  |        |  |
| 09/01/96          | LABOR DAY              |   |  |        |  |
| 11/28/96          | THANKSGIVING DAY       |   |  |        |  |
| 11/29/96          | DAY AFTER THANKSGIVING |   |  |        |  |
| 12/24/96          | CHRISTMAS EVE          |   |  |        |  |
| 12/25/96          | CHRISTMAS DAY          |   |  |        |  |

## TENANTS

This report lists all tenant names and numbers defined in the system. A sample screen follows:

```
[tentrpt]      Tenant Master Report

Ready to produce Report. Okay to continue? (Y/N)[Y] █
```

## TENANTS — SAMPLE REPORT

05/04/96 TRADE CENTER MAIN Page 1  
09:07 Tenant Report

| Number | Description                 |
|--------|-----------------------------|
| 1      | WESTWOOD SECURITY SYSTEMS   |
| 2      | SOS PUBLISHING (CALIFORNIA) |
| 3      | BETA SOFTWARE               |
| 4      | WALKINS PRODUCTS, INC       |

## COMPANY, DEPT, LOCATION, JOB CAT

These reports list user-defined company, department, location and job category information. The report screens are identical for all four — a sample follows:

```
[comprrt] Company Master Report

Ready to produce Report. Okay to continue? (Y/N)[Y]
```

## COMPANY, DEPT, LOCATION, JOB CAT — SAMPLE COMPANY REPORT

03/25/96 Security Electronics Page 1  
08:41 Company Master List

| Number | Description            |
|--------|------------------------|
| 1      | DRAYTON ENGINEERING    |
| 2      | SMITH-JONES WAFER FAB. |
| 3      | MCDOWELL PUBLICATIONS  |

## INSTRUCTIONS

This report lists the operator instructions to be taken following specified events occurring at specified points. A sample screen follows:

```
[instrprt] Instruction Master Report

Lower Limit Upper limit
Point ID : 2
Zone = :
Tenant :

Sort Sequence: 1) Zone, Point ID
               2) Point ID
```

**SAMPLE INSTRUCTIONS**

| Point             | Point Description   | Zone                    | Instructions   |
|-------------------|---------------------|-------------------------|--|
| 03/25/96<br>08:45 |                     | General Electronics Co  | Page 1   |
|                   |                     | Instruction Master List |  |
| 7114              | PRIORITY 10 ALARM   | 4                       | EVACUATE LAB AREA<br>NOTIFY BUILDING MANAGER PAGER #12345<br>DIRECT FIRE CREW TO SCENE<br>PROVIDE ASSISTANCE AS NECESSARY<br>LOG EVENT START/STOP IN SHIFT LOG |
| 9011              | RDI 808 #1 1.1 FIRE | 5                       | REMOTE SITE FIRE ALARM<br>CALL 777-1212 AND NOTIFY LOCAL FIRE DEPT<br>NOTIFY OPERATIONS MANAGER PAGER #12345<br>LOG EVENT IN SHIFT LOG BOOK                    |

**MAPS**

The map report lists all points incorporated into user-defined system maps. The report screen prompts only for the desired sequence: point ID, point type, or map name.

**SAMPLE REPORT — MAP INFORMATION**

| Point             | Point Type | Map Name              |
|-------------------|------------|-----------------------|
| 03/25/96<br>09:33 |            | CAMPBELL TECHNOLOGY   |
|                   |            | Map Definition Report |
| 1                 | CAMERA     | HLP_PNTS              |
| 1                 | DOOR       | HLP_DOOR              |
| 2                 | DOOR       | HLP_DOOR              |
| 2                 | SENSOR     | HLP_PNTS              |
| 3                 | ALARM      | HLP_PNTS              |

**DEVICE CONFIGURATION REPORTS****ZONES**

This report lists all zones defined in the system. A sample screen follows:

```

|zonerprt|      Zone Master Report
Ready to produce Report Okay to continue? (Y/N)[Y] █

```

**ZONES — SAMPLE REPORT**

| Zone | Description          | Area | Prim | Level |
|------|----------------------|------|------|-------|
| 1    | ALPHA LAB ZONE       | P    | H    | G     |
| 2    | HARD PASSBACK ZONE 2 | P    | H    | L     |
| 3    | HARD PASSBACK ZONE 3 | P    | H    | L     |
| 4    | HARD ANTI PASSBACK   | V    | H    | G     |

**POLLERS**

The report lists all defined pollers in the system. A sample screen follows:

```
[pol_rptL]      Poller Master Report

                Lower Limit  Upper Limit
Point ID   :    3
Poller Type:
Zone       :
Tenant     :

Sort Sequence      1) Point ID
                   2) Point Type, Point ID
                   3) Point Key
                   4) Zone, Point ID
```

**POLLERS — SAMPLE REPORT**

| Poller | Date In            | Comp # | Poll # | Prim | Poller Type Desc | Disabled | Zone | Zone Desc |
|--------|--------------------|--------|--------|------|------------------|----------|------|-----------|
| 2      | DATABASE POLLER    | 0      | 0      | 11   | Database         | NO       | 0    | OUTSIDE   |
| 3      | 422/808 POLLER 1   | 0      | 1      | 6    | 808              | YES      | 0    | OUTSIDE   |
| 4      | 808/422 POLLER 2   | 0      | 2      | 6    | 808              | NO       | 0    | OUTSIDE   |
| 5      | 708P PARK POLLER 5 | 0      | 5      | 8    | Parking          | NO       | 0    | OUTSIDE   |

**DEVICES**

This report lists all devices defined in the system. A sample screen follows:

```

[dev_rprt]      Device Master Report

                Lower Limit  Upper Limit
Device ID   :   3
Device Type:
Zone       :
Tenant     :

Sort Sequence      1) Point ID
                   2) Device Type Point ID
                   3) Point Key
                   4) Zone, Point ID

```

### DEVICES — SAMPLE REPORT

```

03/25/96          McCartney Foundation          Page 1
08:50             Device Master Report

```

| Device | Device Desc    | Comp # | Poll # | Address | Prim | Device Type | Desc | Disabled | Zone | Zone Description      |
|--------|----------------|--------|--------|---------|------|-------------|------|----------|------|-----------------------|
| 1      | HOST           | 0      | 0      | 0       | 1    | Host        |      | NO       | 0    | OUTSIDE               |
| 10     | LC #1          | 1      | 0      | 0       | 2    | Controller  |      | NO       | 0    | OUTSIDE BUILDING      |
| 100    | DIAL-UP 422 #1 | 100    | 0      | 1       | 15   | SE422       |      | YES      | 0    | OUTSIDE BUILDING      |
| 801    | BETA 808 SX# 2 | 0      | 2      | 2       | 10   | 808SX/SN    |      | NO       | 2    | HARD PASS BACK ZONE 2 |
| 802    | BETA 804S #1   | 0      | 2      | 1       | 4    | 808S        |      | NO       | 2    | HARD PASS BACK ZONE 2 |

### READERS

This report lists all readers defined in the system. A sample screen follows:

```

[rdr_rprt]      Reader Master Report

                Lower Limit  Upper Limit
Reader ID   :   3
Zone Number :
Tenant Number:

Sort Sequence      1) Reader ID
                   2) Reader Key
                   3) Zone, Reader Key

```



**AUTO OPENS / ACTIVATES**

This report lists system points and readers which have auto-open or auto-activate times. A sample screen follows:

```
[autorprt]      Auto Open/Activate Report

                Lower Limit  Upper Limit
Point ID  :      3
Tenant   :
```

**AUTO OPEN / ACTIVATE — SAMPLE REPORT**

| 03/25/96<br>08:54 |                     | Security Electronics<br>Auto Open/Activate Master List |      |       |       |     |     |     |     |     |     | Page 1 |     |
|-------------------|---------------------|--|------|-------|-------|-----|-----|-----|-----|-----|-----|--------|-----|
| Point             | Point Description   | Point Type   | Tmcd | Start | End   | Mon | Tue | Wed | Thu | Fri | Sat | Sun    | Hol |
| 1830              | 818 #7 DOOR #3 +VIP | READER   | 9    | 10:35 | 10:40 | Y   | Y   | Y   | Y   | Y   | N   | N      | N   |
| 1850              | 818 #7 DOOR #5      | READER   | 14   | 11:29 | 12:31 | Y   | Y   | Y   | Y   | Y   | N   | N      | N   |
| 1870              | 818 #7 DOOR #7      | READER   | 16   | 11:59 | 13:01 | Y   | Y   | Y   | Y   | Y   | N   | N      | N   |
| 8240              | TIM'S 804S DOOR 4   | READER   | 6    | 15:39 | 15:39 | Y   | Y   | Y   | Y   | Y   | N   | N      | N   |

**808 REPORT DEFINITION**

This report lists all action reports defined for the system 800-series ACUs. A sample screen follows:

```
[rdefrprt]      808 Definition Report

Ready to produce Report. Okay to continue? [Y/N](Y)
```

**808 REPORT DEFINITION —SAMPLE REPORT**

| 03/05/96<br>15:22       |                | Security Electronics<br>808 Report Definition |                          |              |  | Page 1 |  |
|-------------------------|----------------|---|--------------------------|--------------|--|--------|--|
| 100                     | DIAL-UP 808 #1 | Report  | 1                        |              |  |        |  |
|                         |                | Send To Host                                  | Close Latch              | Close Output |  |        |  |
| Bldg Open               |                | Y   | N                        | Y            |  |        |  |
| Bldg Limited            |                | Y   | N                        | Y            |  |        |  |
| Bldg Closed             |                | Y   | N                        | Y            |  |        |  |
| Time Code               |                | 1   |                          | 1            |  |        |  |
| Time Code               |                |   |                          |              |  |        |  |
| Time Code               |                |   |                          |              |  |        |  |
| Contact Number          |                |   |                          |              |  |        |  |
| Print Asterisk With Log |                | N   | Prevent Building Closure | N            |  |        |  |

## 808 DEVICE CONFIGURATION

This report lists configuration information for the system 800-series ACUs. A sample screen follows:

```
[dconprt] 808 Device Configuration Report
Ready to produce Report. Okay to continue? [Y/N](Y) █
```

## 808 DEVICE CONFIGURATION — SAMPLE REPORT

| 06/05/96           |              |          | Simms Oil Corporation    |                |                       |
|--------------------|--------------|----------|--------------------------|----------------|-----------------------|
| 15:25              |              |          | 808 Device Configuration |                |                       |
| 100 DIAL-UP 808 #1 |              |          |                          |                |                       |
| Level              | Name         | Password | Reports                  | Key Definition |                       |
| A                  | OPERATOR MGR | NEW      | Tamper                   | 9              | Primary Key Type 1060 |
| A                  | G. SAYLES    | SAYLSG   | Power Fail               | 4              | Aux. Key Type NONE    |
| B                  | LYNN VAUGHAN | LYNSID   | Override                 | 1              | Facil Code *          |
| C                  | TIM JONES    | TJO123   | Alt Facil Code           | A000           |                       |

## DIALERS

The two dialer report types detail the remote dialup interface (RDI) devices defined for the system or those RDI devices which have experienced communication trouble. A sample screen follows:

```
[dialrprt] Dialer Report
Report Option 0 1) All
              2) Trouble
```

## DIALERS — SAMPLE REPORT

| 03/25/96 | Security Electronics |               |           |           |            | Page    | 1          |
|----------|----------------------|---------------|-----------|-----------|------------|---------|------------|
| 09:00    | Dial Master Report   |               |           |           |            |         |            |
| Device   | Device Description   | Remote Number | Last Date | Last Time | Who Called | # Trans | # Failures |
| 900      | RDI - ALPHA LAB      | 4921342       | 02/19/94  | 17:10     | Host       | 0       | 1          |

## SITE DEFINITION

This report lists all site groups and codes defined for the system. A sample screen follows:

```
[siterprt]   Site Code Master Report

Ready to produce Report.  Okay to continue? (Y/N)[Y] █
```

### SITE DEFINITION — SAMPLE REPORT

```
03/25/96                Security Electronics                Page 1
09:02                   Site Code Master Report

Group      Code
-----
   1        0000
  100       1000
  101       1001
 6016       7279
```

### ABA CONFIGURATION

This report lists all the ABA configurations defined for the system, and gives the configuration parameters. A sample screen follows:

```
[abacrpert]   ABA Configuration Master Report

Ready to produce Report.  Okay to continue? (Y/N)[Y] █
```

### ABA CONFIGURATION — SAMPLE REPORT

```
03/25/96                Security Electronics                Page 1
09:17                   ABA Configuration Report

Configuration ID      1000
                    Start  Length
Key  A                1      3
Key  B                4      2
Key  C               10      3
Expiration Date Start      15  Site Code Start      20
ABA Key Data Action      0

                                Deny Access      During Fail Soft
                                Deny Access

Based on key number          N                    N
Based on site code          N                    N
Based on expiration date    N                    N
Use site code as key        N                    N
```

## DKR CONFIGURATION

The reports lists the system default DKR parameters. A sample screen follows:

```
[dkcrprtl]    DKR Configuration Master Report

Ready to produce Report.  Okay to continue? (Y/N)Y|
```

## DKR CONFIGURATION — SAMPLE REPORT

| 06/12/96   |           | Lotus Refineries         |                 |           |              |     | Page 1 |               |     |       |                 |     |       |
|------------|-----------|--------------------------|-----------------|-----------|--------------|-----|--------|---------------|-----|-------|-----------------|-----|-------|
| 15:21      |           | DKR Configuration Report |                 |           |              |     |        |               |     |       |                 |     |       |
| Config. ID | Send Once | Read Range               | Number of Reads | Read Time | Beeper Times |     |        | Red LED Times |     |       | Green LED Times |     |       |
|            |           |                          |                 |           | On           | Off | Total  | On            | Off | Total | On              | Off | Total |
| 1          | Y         | 255                      | 1               | 100       | 20           | 30  | 20     | 0             | 0   | 0     | 0               | 0   | 0     |

## SE 422 PIN MASTER REPORT

This report lists keyholders having system-calculated SE 422 PIN numbers. A sample screen follows:

```
[p422rprt]    SE/422 PIN Master Report

Keyholder ID      : 0          Lower limit Upper Limit
Company          : 0          999999999
Dept             : 0          9999
Location         : 0          9999
Jobcat           : 0          99999
Issue Date       : ***** 01/25/94
Key Number       : 0          999999999
Shift            : ****      2222
Emp Stat         : ****      2222
Tenant           : 0
Extended Info ?  : N
```

**SE 422 PIN MASTER REPORT — SAMPLE**

| 03/25/96<br>09:22 |         | Soames Industries<br>SE/422 Quick List |      |        |       | Page 1    |              |        |
|-------------------|---------|--|------|--------|-------|-----------|--------------|--------|
| Keyholder         | Key No  | Keyholder Name                         | Dept | Jobcat | Phone | Title     | Loca Floor   | 422Pin |
| 6109              | 1895573 | Duane Eddie                            | 1    | 3      |       | Assembler | Main Mfg Flr | 60030  |
| 6110              | 1784422 | Juarez Sandi                           | 1    | 3      |       | Assembler | Main Mfg Flr | 31949  |
| 6112              | 1901112 | De Witt Charles                        | 1    | 3      |       | Assembler | Main Mfg Flr | 32112  |
| 6113              | 1788122 | Ames Linda                             | 1    | 3      |       | Assembler | Main Mfg Flr | 35976  |

**132-COLUMN REPORT DISPLAY**

The local print program was originally written to accommodate an 80-character terminal display. Some terminals now use up to 132 characters, and the new *132-Column Report Display* feature allows for this. The terminals are: HP700/44; HP700/92; Color PC terminals using *Reflections 4* terminal emulation software. The feature is automatically enabled, and automatically resumes the 80-character display mode when the user exits the report program. A sample 132-character display follows:

**NOTE**

1. When in the 132-column mode, the terminal scrolls one half page at a time.
2. This new feature is not supported by the HP console terminal provided with the host and LC systems.

**132-COLUMN REPORT — SAMPLE DISPLAY**

| Point | Point Description  | Zone | Date     | Time     | Access Type            | Keyholder | Keyholder Name | Key No  |
|-------|--------------------|------|----------|----------|------------------------|-----------|----------------|---------|
| 8110  | TIM's 808SX DOOR 1 | 801  | 11/18/96 | 07:28:26 | PROJECT ACCESS GRANTED | 123456789 | TIM H+P+SMF    | 5825175 |
| 8110  | TIM's 808SX DOOR 1 | 801  | 11/18/96 | 07:28:06 | INVALID PROJECT        | 123456789 | TIM H+P+SMF    | 5825175 |
| 8110  | TIM's 808SX DOOR 1 | 801  | 11/16/96 | 08:32:58 | PROJECT ACCESS GRANTED | 123456789 | TIM H+P+SMF    | 5825175 |
| 8110  | TIM's 808SX DOOR 1 | 801  | 11/16/96 | 08:22:10 | PROJECT ACCESS GRANTED | 123456789 | TIM H+P+SMF    | 5825175 |

# SECTION 6

# SYSTEM ADMINISTRATION

## INTRODUCTION

The administration functions are used to control and maintain the system. These functions are accessed from the system administration menu, [sys\_menu], via the main menu. (Depending on the operator's program security level, some or all of these functions may not be available.) A sample screen follows:



## SECTION ORGANIZATION

The procedures in this section are in the order shown in the system administration menu (above). The associated subscreens also follow in order. After the current screen has been saved, most subscreens display by pressing F2 but some display automatically.

## ADDITIONAL INFORMATION

Additional system administration-related information is provided at the conclusion of this section.

## ADD USERS [addusers]

The add users screen, [addusers], is entered to add, change, or delete system users / operators.

### IMPORTANT

The administration log-on and password must be used to access this screen. If you are already logged on with your regular password, first log off in the normal way, then log on again using the administration log-on and password.

A sample [addusers] screen follows:

```

[addusers]                               User Entry Program
1) User Name:                             [      ]
2) Keyholder Id:                           [      ]
3) Program Security Level:                 [  ]
4) Tenant Number:                          [  ]
5) Monitoring Group:                       [      ]
6) Monitoring Security Level:              [  ]
7) Allow Alarm Servicing:                  [  ]
8) Jump Alarm Servicing:                   [  ]
9) Jump Timer Servicing:                   [  ]
10) Language (1..9) :                      [  ]
11) Real-Time Maps Security Level:         [  ]
Enter the Login name of the user or press F1 to exit.
1) EXIT 2) 3) 4) 5) 6) 7) 8)

```

**User Name.** Required. Enter the user name (first eight letters of last name recommended).

**Keyholder ID.** Optional. User's keyholder ID. Default is 0. You should have a keyholders ID assigned to you. When you enter this menu, your name is displayed at the top of the screen.

- ③ **Program Security Level.** Optional (range 1—9999). Code number indicating the specific screens the user can access. Default is 1 (complete access).
- ④ **Tenant.** Optional. Enter tenant number (if applicable). Default is tenant 0.
- ⑤ **Monitoring Group.** Optional. System code indicating transaction types available to this user. Default is \* — All transaction types.

Transactions may be defined as elements of monitoring groups. For example, access granted transactions could be placed in monitoring group A, door forced open transactions could be placed in monitoring group B, all other transactions could be placed in monitoring group 0 (zero)—the field default. Assignments for these groups could be:

Group A — Assigned to those who need only to monitor day-to-day access granted transactions.

Group B — Assigned to security guards who need to see all door forced open transactions.

Group 0 — Assigned to the system administrator who needs to see all transactions.

- ⑥ **Monitoring Security Level.** System code (0, 1, or 2) indicating the user's monitoring / data changing capabilities. Monitoring security level 0 allows full monitoring / changing capabilities, including disabling points and halting pollers. Monitoring security level 1 is recommended for general use, since it permits a user to control certain functions, such as doors, but not pollers and points. Monitoring security level 2 limits users to a purely observational capacity; no functions can be controlled.

#### IMPORTANT

1. We recommend that level 0 be assigned only to completely trained and responsible personnel, since some level 0 operations could easily disable the system if not performed correctly.
2. Enter **C** in this field to use the new enhanced security monitoring feature (see *Enhanced Monitor Security* below).

- ⑦ **Allow Alarm Servicing.** **Y / N / F** field indicating if the user has the authority to respond to alarms in the monitor program, or enter **F** if the alarm fast acknowledgment feature is to be allowed.
- ⑧ **Jump Alarm Servicing.** **Y / N** field indicating if the user has the authority to automatically jump to alarm servicing from monitor when an alarm occurs.

- 9 **Jump Timer Servicing.** Y / N field indicating if the user has the authority to automatically jump to timer servicing from monitor when a timer event occurs.
- 10 **Language.** The code number entered will determine what language the system will use for this user. Valid choices are 1=English, 2=French.
- 11 **Real-Time Maps Security Level.** 0=Complete functionality, 2=View maps only (no control capabilities).

## MODIFY PASSWORDS [mod\_pass]

Use the modify password screen to change an existing password (must be logged in as *addusers*). Enter the user name, then follow screen prompts. A sample screen follows:

```
[mod_pass]          Modify Passwords

Enter User Name or press ENTER to exit:  tim
Setting password for user:  tim
Last successful password change for Lim: Mon Oct 16 13:53:28 1995

          Choose password

You can choose whether you pick a password,
or have the system create one for you.

    1. Pick a password
    2. Pronounceable password will be generated for you

Enter choice (default is 1):
```

Enter the password twice to confirm it.

### NOTE

If you enter a user name but then decide that the password does not need to be changed, then the current password must be reentered.

To return to the system administration menu after the new password has been entered, first press **Enter** to return to

```
[mod_pass]          Modify Passwords

Enter User Name or press ENTER to exit:
```

then press **Enter** again.

## PROGRAM SECURITY [sec\_menu]

### PROGRAM SECURITY LEVEL ENTRY [pgacentr]

Begin creating program security level types by first displaying the program security level entry screen [pgacentr]:

```
[pgacentr]          Program Security Level Entry
  ① Security Level Number: 28    ② Description: NEW KEYS ONLY / MONITOR
                                     █

PRESS <F2> <NEXT FORM> TO DEFINE PROGRAM SECURITY FOR THIS LEVEL
```

① Enter the security level number (four digits maximum).

② Enter a description (30 characters maximum).

Press F6 Store, then press F2 for the program security level definition screen

### PROGRAM SECURITY ENTRY DEFINITION [pg1\_entr]

```
[pg1_entr]          Program Security Level Definition  *Allowed Functions*
                                     (Y/N)
Program Name and Description          Add Update Delete
█
```

Press F7; the first six system data items display:

```
[sec_zoom]  Program Name Display

Program Name:      Description
ID1_entr - ID Security User Entry
ID1_rpt - ID Security Report
ID2_entr - ID Security Group Entry
ID_menu = ID Security Maintenance
aasmenu = Access Assignments
ahacentr = ABA Configuration Entry
```

Arrow down to the first system item for this new security level; press F1. The system displays the program name and description to the left, and the add/update/delete fields to the right. For example:

| [pg1_entrl]                        | Program Security Level Definition | *Allowed Functions*<br>(Y/N) |        |        |
|------------------------------------|-----------------------------------|------------------------------|--------|--------|
| Program Name and Description       |                                   | Add                          | Update | Delete |
| <b>agrpentrl</b> Access Assignment |                                   | N                            | N      | N      |

Enter Y or N in the add/update/delete fields to give or deny access to these functions on the selected screen. If you do not make any Y/N selection in the Add, Update, and delete fields, the keyholder will not have access to the screen. Press F6 Store and then, before any other action is taken, press F5 to return to the add mode for the next entry. Repeat these actions for all items in the new security level. Note that the Add, Update, Delete fields only apply to screens with this capability not to menus.

#### NOTE

1. Add items to an existing program security using the foregoing methods.
2. To delete an item, first select as shown above then use Esc, d, r.

| [pg1_entrl]                        | Program Security Level Definition | *Allowed Functions*<br>(Y/N) |        |        |
|------------------------------------|-----------------------------------|------------------------------|--------|--------|
| Program Name and Description       |                                   | Add                          | Update | Delete |
| <b>agrpentrl</b> Access Assignment |                                   | N                            | N      | N      |

### COPY SECURITY [mnaccopy]

It may be easier to copy an existing security level and make changes to this when creating a new security level. To do this, display the [mnaccopy] (Copy Program Security) screen, enter the existing security level number in the Copy From field and enter the new security level number and description in the Copy To field. Make changes to the new security level using the above procedures.

|             |                       |
|-------------|-----------------------|
| [mnaccopy]: | Copy Program Security |
| Copy From - | █                     |
| Copy To :   |                       |

### SECURITY MASTER LIST [pgacrprt]

Use the security master list [pgacrprt] facility to print a listing of all security levels established for your system or those for a selected range. A complete list is given in *Appendix D: Program Security Master List*.

```
[pgscrpt1] Security Master List.
          Lower Limit Upper Limit
Security Level : 3
```

## DISPLAY ALL VALID LOGINS [showuser]

Use the [showuser] screen to identify — by hard copy printout or report display at the system terminal — all operators who have access to the system (use the [showwho] (Display All Valid Logins) screen to display operators currently logged on. Follow prompts when the screen displays. A sample report is recreated below:

```
10/23/96          Eton Engineering          Page 1
13:02

Login Name       Tenant    Security    Keyholder
-----
anderson         0        1           1123456
melville        0        1           1334229
smith           0        1           1348876
```

## DISPLAY CURRENT DATE AND TIME [showdate]

Use the [showdate] screen to display the current system date and time. A sample display follows:

```
[showdate]      Display Current System Date
Feb Oct 28 09:14:00 PDT 1995
Press RETURN to continue.
```

## DISPLAY ALL USERS WHO ARE LOGGED IN [showwho]

Use the [showwho] screen to display operators currently logged in (use the [showuser] screen to identify all operators who have access to the system). Follow prompts when the screen displays. A sample report is recreated below:

```
[showwho]      Display All Currently Logged in Users:
address:      tty01          Oct 28 09:11
tca          tty02          Oct 28 09:11
root         tty03          Oct 28 09:13
root         tty04          Oct 28 09:12
```

## PURGE A PENDING REPORT [purgrprt]

Use this feature to halt a report currently being printed (applies only to reports created under your ID). The feature can also be used to display reports. Note that if you log on using addusers you will have complete printer control.

## ENABLE TERMINALS FOR GLOBAL BEEPING [beepentr]

This feature is used to enable terminals to beep when an alarm occurs. Obtain terminal IDs (port connection — `tty___`) from system installer and enter with optional description.

```

[beepentr] Enable Terminals For Global Alert

Terminal      Terminal Description      Alert
TTY
tty01        CONSOLE                    Y
  
```

## SYSTEM CONFIGURATION (syclmenu)

### CONTROL FILE MAINTENANCE [ctrlentr]

For informational / custom reporting purposes, certain field titles that display in keyholder record screens [key\_entr] and [key1entr] can be changed to suit the individual user. Since keyholder records may be considered the primary data items for an access control system, many SE 6000 owners use the field title change feature to tailor the system to their precise requirements. Change fields A through F and 1 through 7 as required.

**TERMINAL AUTO SWITCH [ctrlentr].** An additional field at the foot of this screen is optionally used to set up a particular terminal to automatically switch to the alarm servicing screen (from monitor) when an alarm occurs. A sample screen follows:

```

[evenentr]      Control File Maintenance
Company Name:  Security Electronics

Field titles:  Enter "unused" for fields not required
Fields on Page 1 of the Keyholder Entry screen:
  A: Company      B: Dept      C: Location
  D: Job Cat      E: Shift      F: Status

Fields on Page 2 of the Keyholder Entry screen:
  1: Jnr1         2: Jnr2         3: user3
  4: Jnr4         5: Jnr5         6: user6
  7: Remarks

Terminal to auto-switch for Alarm Servicing: 11401

```

## EVENTS [evenentr]

The task / event subsystem is used to program one or more tasks to be automatically performed in response to the occurrence of a user-defined event. Tasks and events are linked, and the task must be entered and stored before the system allows the creation of a related event. Events can initiate the same task, or a single event can initiate multiple tasks. Events controlled by a time code automatically perform the task entered in the activate field at the start of the code and the task entered under the deactivate code at the end of the time code. A sample screen follows:

```

[evenentr]      Event Entry
1 Event Serial # -
2 Event Point ID - 
3 Transaction Type: 3
4 Modifier       : 3 - NEGATIVE ACKNOWLEDGE
5 Event Date     : *****      Event Time: *****
6
7 Time Code      : 0 00:00 - 00:00  1  4  1  4  1  4  1  4
8 Perform Task ID :      =

```

**Event Serial #.** System-assigned. Keeps track of all event entries.

**Event Point ID.** Required. The point ID at which a specified transaction must occur to initiate a task (can be time code or event date initiated).

**Transaction Type.** Required. The transaction number which must occur at the specified point ID to generate a task (see *Appendix C: System Transactions* for a list of the system-generated transactions numbers).

**Modifier.** Optional. If applicable, the transaction modifier which defines the event if the message is user-defined.

**Event Date.** Optional. If the task referenced by this event is to be system-initiated, enter the applicable date.

**Event Time.** Optional. If the task referenced by this event is to be system-initiated, enter the applicable time.

**Time Code.** Optional. If the task referenced by this event applies to a specific time code, enter the time code number.

**Perform Task ID.** Required. Enter the task ID number.

## TASKS [taskentr]

Used to set up tasks for the task / event subsystem. Tasks must be created before the associated event.

| Task Entry |                                       |
|------------|---------------------------------------|
| 1          | Task Serial # :                       |
| 2          | Task ID # : <input type="text"/>      |
| 3          | Description :                         |
| 4          | Task Point ID :                       |
| 5          | Activate Code :            Extension: |
| 6          | Deactivate Code:           Extension: |
| 7          | User Interactive: N                   |

**Task Serial #.** System-assigned number used to keep track of all tasks.

**Task ID.** Required. Enter a user-assigned task ID number. Task IDs do not have to be unique. All occurrences of a given task will be executed by an associated event.

**Description.** Optional. Enter a brief description of the task.

**Task Point ID.** Required. Point ID number controlled by this task.

**Activate Code, Extension.** Required. System code number for the type of action to be performed. The extension applies to camera presets for pan and tilt, or image verification when used with a Polaroid ID-4000 system. See table following this field description list.

**Deactivate Code, Extension.** Optional. If this task is to be automatically controlled by a time coded event, enter the activate / deactivate code to be executed when the event time code ends. See table following this field description list.

**User Interactive.** Conditional (applies to event times). A Y/N field to indicate if a timed task can be cancelled by an operator.

#### ACTIVATE / DEACTIVATE CODES

|    |                      |  |
|----|----------------------|--|
| 09 | REQ MANUAL ACCESS    | Request to perform manual access.  |
| 29 | FORGIVE PASSBACK     | Request to forgive passback.   |
| 41 | MANUAL UNLOCK        | Unlock a sensor / lock for an unlimited time.  |
| 45 | MANUAL LOCK          | Lock a sensor /lock.   |
| 46 | TIME UNLOCK          | Unlock a sensor / lock for the amount of time specified by the hardware settings, or, where applicable, by the amount of time in the <i>Unlock Time</i> field of the reader entry screen.  |
| 56 | BUILDING OPEN        | Set building mode to OPEN  |
| 57 | BUILDING LIMITED     | Set building mode to LIMITED   |
| 58 | BUILDING CLOSED      | Set building mode to CLOSED  |
| 70 | DEACTIVATE OUTPUT    | Turn off the specified output. Use this code if you are elsewhere turning an output on for an unlimited time.  |
| 71 | ACTIVATE OUTPUT      | Turn on a specified output for the amount of time shown in the <i>Time</i> field on the point entry screen. If <i>Time</i> =0, the output will be on for an unlimited amount of time, and you must turn it off with an a deactivate output code. |
| 80 | Chain Task           | Jumps to another group of task records and is used to consolidate multiple task into a separate task.  |
| 81 | EXTENDED PROCESSING  | Instruct extended processing poller to process a transaction. Use with elevator, parking control, VIP2, and poller transactions with a point ID which matches the poller record for these functions.   |
| 89 | SHUNT POINT          | Shunt a specified point.   |
| 90 | UNSHUNT POINT        | Unshunt a specified point.   |
| 91 | REQUEST RESET DEVICE | Perform a device reset for an applicable device.   |
| 92 | REQUEST RESET KEYS   | Perform a key download for an applicable device.   |

|     |                               |   |
|-----|-------------------------------|---|
| 100 | ACTIVATE PROJECT              | Activate an inactive project.   |
| 101 | DEACTIVATE PROJECT            | Deactivate an active project.   |
| 102 | NORMALIZE or<br>CLEAR PROJECT | Change project status to its normal condition (clears an override condition). |

### TASK EVENT / MASTER REPORT [taskrprt]

This report shows all tasks / events established in the system:

| Task   | Task Description | Point  | Activate Desc       | Deactivate Desc     | Cancelable                      |
|--------|------------------|--------|---------------------|---------------------|---------------------------------|
| 42     | UNLOCK DOOR      | 708 #2 | ENTER ZONE B        | Man Open            | N                               |
| EVENTS |                  | 7120   | 708 #2 ENTER ZONE B | 62 0 KEY NOT ACTIVE | No Activity                     |
|        |                  | Tmcd   | Start               | End                 | Mon Tue Wed Thu Fri Sat Sun Hol |
|        |                  | 1      | 15:30               | 16:15               | Y Y Y Y Y N N N                 |

### TRANSACTIONS [tranentr]

Customized versions of any system transaction (log message) can be created. The custom transactions are created using the transaction entry screen, where they are linked to the point or reader screens by a transaction modifier code. The codes are any of the following: A — Z (uppercase), a — z (lowercase), 1 — 9 (0 is the default modifier for all standard transactions). (Up to 62 log messages can be associated with the same event.)

```

[tranentr]      Transaction Entry
1 Transaction Type (ID): 1      2 Transaction Modifier: A
3 Transaction Group : *      4 Alarm Priority : 0
5 Event/Task Activity: 0     6 Time To Acknowledge: 0
7 Display Color: 2          8 Clear Transaction : ***
9 Monitor Group: 0         10 Printer Color: 0
11 Display Icon :          12 Printer Group: 0
13 Audible Alert: N <Enter 'N' if using Global Beep>
14 Transaction Log : Y     15 Keyholder Log: Y     16 Point Log: Y
17 Description: DAYTIME ACCESS GRANTED

```

**Transaction Type (ID).** The unique ID number of a transaction. The system is pre-programmed to use specific transaction types for certain events at certain types of points. (See *Appendix C: System Transactions* for a complete list of standard transactions.)

**Transaction Modifier.** Required as applicable. Enter a transaction modifier code to indicate a customized version of a standard transaction. The values are: A through Z (all uppercase), a through z (all lowercase), 0 through 9.

**Transaction Group.** For future use. Will permit the categorizing of transactions into broader groups for easier reporting and editing.

**Alarm Priority.** Conditional. Used to declare that a particular transaction is an alarm transaction, and to indicate the alarm priority. The range is 1 through 9, with 1 being the highest priority and 9 the lowest. Enter 0 for a non-alarm transaction.

**Event/Task Activity.** Conditional. Used if the system has been programmed to respond to a particular event via the event / task subsystem. Enter 1 to activate the task; enter 2 to deactivate the task.

**Time to Acknowledge.** Enter a value in minutes to allow for alarm acknowledgment. If the alarm is not acknowledged by this time, an ALARM NOT ACKNOWLEDGED message is written to the log and repeats at the interval specified until acknowledged.

**Display Color.** Determines the transaction display color in the monitor mode. The colors are:

- 0 = Black
- 1 = Red
- 2 = Green
- 3 = Cyan (light blue)
- 4 = Blue

**Clear Transaction.** Conditional. Enter the alarm clearing transaction number. For example, with transaction 92 (Alarm Active), enter 93 (Alarm Clear) as the clearing transaction. If a clearing transaction is specified, the alarm event cannot be removed from the pending alarms screen until the clearing transaction is received.

**Monitor Group.** Used to classify transactions into groups, so that the display of transactions based on log-in name can be controlled. The default monitor group assignment when users are added to the system is \* — All monitor groups displayed.

**Printer Color.** Determines the color in which this transaction will display when printed on a color-capable log printer. The colors are:

- 0 = Black
  - 1 = Red
-

- 2 = Green
- 3 = Cyan (light blue)
- 4 = Blue

**Display Icon.** For future use.

**Printer Group.** Each log printer must include the selected printer group in its list of available printer groups. If the selected printer group is not included, the transaction will not be printed on the log printer. Printers are preset to include all transactions (Printer Group=\*). To prevent a transaction from printing, assign it to a printer group other than 0, then change the printer to 0.

**Audible Alert.** Indicates with **N** (none), **S** (single), or **C** (continuous) the type of audible alert which this transaction should produce (applies only if a user is in the monitor mode). If you wish to have a terminal alerted whenever this transaction occurs, enter **N** in this field.

**Transaction Log.** **Y/N** field to indicate if this transaction is to be stored in the archive history file on disk. The transaction history file is listed using the transaction history report.

**Keyholder Log.** **Y/N** field to indicate if this transaction is to be stored in the keyholder history file on disk. The system keeps a small area of disk space available to store the last 20 events for all individual keyholders in the system. The keyholder history file is listed using the keyholder history report.

**Point Log.** **Y/N** field to indicate if this transaction is to be stored in the point history file on disk. The system keeps a small area of disk space available to store the last 20 events for all individual points in the system. The point history file is listed using the point history report.

**Description.** Used to define the transaction description displayed on the monitor screen.

---

## DATABASE MAINTENANCE [db\_menu]

---

### DISPLAY DATABASE STATISTICS [dbstats]

Display this data regularly to control disk space usage. Note the PUBLIC.archist table size near the end of the report. The table size indicates the number of transactions currently stored. Perform an archive whenever the row count is roughly 80% of the expected number of rows.

A message is displayed if the row count reaches the expected number of rows. If this happens, archive immediately. Two other tables should be checked regularly and purged if the expected number of rows exceeds 80%: PUBLIC.download; PUBLIC.almtran.

### PERFORM BACKUP [bkup]

Two backup types are available — Database and Full Volume:

---

```

[Backup]                               Backup System

0) Exit - Return to Previous Menu
1) Data Base Backup
2) Full Volume Backup

Which backup do you wish to perform ?

```

**DATABASE BACKUP.** A database backup copies all information in the database (exceptions user and map information). If you make a number of changes to keyholder, hardware, and / or access information in a single day, then the database backup should be performed each day. For these purposes, use two alternating tapes (one for odd days, one for even) to guarantee that no information will be lost in the event of a hardware malfunction.

**FULL VOLUME BACKUP.** A full volume backup copies all system data including programs, system configuration information, and user / map information. The backup tape created is used to restore the system in the event of a hardware malfunction. A full volume backup should be performed immediately following system installation, and then on a monthly basis or whenever there has been a major system update or reconfiguration.

### DOWNLOAD CLEAN UP AND RETRY [downcIn]

Download records are data transferred from the database to computer memory or to intelligent remote devices. Each time information is entered and stored in the database, one or more download records are created and written to the download file. If the download transfers are unsuccessful, the number of records created can increase the download file size to a point where system performance is affected, and these records should be first retried then deleted. In general, perform a download cleanup when the PUBLIC.download table reaches 80% of the expected number of rows, or if it has been necessary to make a significant number of database changes. Monitor this table using Display Database Statistics [dbstats].

If you use a large number of intelligent devices, then this table should be checked frequently. A typical time period for cleaning the download table is once per month. Download records are not automatically deleted upon successful transfer.

### ACCESS CONTROL TRANSACTION ARCHIVING [accsarch]

Archiving transfers information from the system hard disk to tape, freeing up space on the hard disk for new data. Archiving should be performed regularly to ensure disk integrity. Perform an archive when the PUBLIC.archist table reaches 80% of the expected number of rows. Monitor this table using *Display Database Statistics* [dbstats]. Archiving is usually performed monthly or every two months. Note that unless necessary for reporting purposes, WSE recommends that you archive system information when your transaction volume reaches 100,000 records.

## ALARM TRANSACTION CLEAN UP [alarmcln]

Each time an alarm is triggered, a record is created and stored in a separate file along with the operator's alarm servicing response. This table is then available for reporting using the alarm servicing report. Over time, the size of this table grows and takes up excessive space on the hard disk. Cleanup this table when the PUBLIC.alrmtran table reaches 80% of the expected number of rows. Monitor this table using *Display Database Statistics* [dbstats].

## JOURNAL ARCHIVE [jourarch]

This function copies journal records to tape and then deletes them from the hard disk. The journal archive program archives all journal information except for the current day. Archiving is performed using the [jourarch] screen:

```
(jourarch)          Offload Audit from Disk

This program will offload the Audit Trail from disk to tape.
WARNING: ANY INFORMATION ALREADY ON THIS TAPE WILL BE LOST !!
*****
Please make sure that the tape is loaded

Do you wish to continue ?
```

## JOURNAL REPORTING [jourrprt]

This function reports all changes to the database. The report prints the column name and value for each field of each record that has been entered. With updates, the report shows the record before and after the change. Associated operator, and date and time are also reported. A sample report follows:

```
04/02/96          De Quincy Laboratories          Page 1
12:14             Audit Trail Report

Operator          Table          Date          Time          Operation Type
-----          -
jon               cards          04/02/96     12:07         Add
upbzone:         -1
ppbzone:         -1
keyisalt:        NULL
priv: N
```

## SPECIAL JOURNAL REPORTING [josprprt]

This function produces a formatted history report of all database changes to the keyholders and keyholder access assignment information. Sample screens and reports follow:

```
[jmsprpt] Special Journal Transaction Report
          Lower      Upper
Transaction Date: **** 03/28/94
Keyholder Id:      0
Use Tape For Reporting: N
```

## KEYHOLDER LOADING [loadmenu]

This function copies keyholder IDs and names from an DOS ASCII file to a Unix then creates keyholder records. The format of records in the ASCII file must be as follows:

- Keyholder ID ^ALastname ^AFirstname (^A refers to a single control-A character)
- Keyholder ID 1 to 9 digits; both name fields 15 characters maximum

## ID SECURITY MAINTENANCE [ID\_menu]

The ID Security Maintenance function controls access to the information shared by the SE 6000 and the Polaroid ID-4000 Identification System. It also controls access to selected fields in the keyholder record. Add/update functions within the key enter and key-1 enter screen can be regulated by user ID.

### ID SECURITY USER ENTRY [ID1\_entr]

ID Security Maintenance data is created via the ID Security Maintenance menu:

```
[ID1_entr] ID Security Entry
1  Username: 1-
2  Security Group: 1
```

Required. Enter the user name.

Required. Enter the user's security group number. With the SE 6000, ID security groups must exist (or be created via the ZOOM function) before the system administrator can complete user entry.

## ID SECURITY GROUP ENTRY [ID2\_entr]

This function is used to create ID security groups. A sample screen follows:

```

[ID2_entr] ID Security Group Entry

1 Security Group Number: 1
2 Security Description: FULL PRIVS

Press Rest F10 for ID Security Fields Screen
  
```

Required. Enter a unique security group number in the range 1—999.

Optional. Enter a group description (30 characters maximum).

## ID SECURITY REPORT [ID1\_rprt]

This function is used to prepare a report showing all users entered into the ID security feature, along with tenant and group definition information. A sample of a partial screen and report follow:

```

[[ID1_rprt] ID Security Maintenance Report

Ready to produce Report. Okay to continue? (Y/N)[Y]
  
```

| Login Name | Tenant | Tenant Name      | Group | Group Name             | Add    | Del |
|------------|--------|------------------|-------|------------------------|--------|-----|
| JERID      | 0      | All Encompassing | 1     | Complete Record Access | Y      | Y   |
|            |        | Field            |       | View                   | Modify |     |
|            |        | Keyholder ID     |       | Y                      | Y      |     |
|            |        | Tenant Number    |       | Y                      | Y      |     |
|            |        | Key Number       |       | Y                      | Y      |     |
|            |        | Company          |       | Y                      | Y      |     |
|            |        | Dept             |       | Y                      | Y      |     |

---

## MISCELLANEOUS INFORMATION

---

### ADJUSTABLE BAUD RATE—708P / 800 POLLERS

Multiple baud rates are supported for the diverse mix of communications equipment available for the SE 6000 system. The baud rate is set by changing the HOSTBAUD parameter in the \$DATAPATH/NPOLLER.x file where x is the associated poller number. The baud rate is entered during installation or changed as needed by the system administrator; operator action is not required. The baud rate options are:

|                   |   |                                   |
|-------------------|---|-----------------------------------|
| Parameter missing | — | HOSTBAUD defaults to 4 (9600 bps) |
| HOSTBAUD=4        | — | 9600 bps                          |
| HOSTBAUD=3        | — | 4800 bps                          |
| HOSTBAUD=2        | — | 2400 bps                          |
| HOSTBAUD=1        | — | 1200 bps                          |
| HOSTBAUD=0        | — | 300 bps                           |

#### NOTE

1. The baud rate set applies to *all* devices controlled by the poller.
2. Though functional, the 300 bps baud rate (HOSTBAUD=0) is not recommended for the 800-series devices. The amount of data downloaded to intelligent ACUs significantly impacts overall system performance when inefficient communication facilities are used.
3. On 708P ACUs, the host port speed on the device is set with dipswitches. Both the device and the poller must be set for the same speed.

### 708P REX SHUNT TIME RESET

The normal operation of a REX switch is to shunt an associated door switch when opening the door from the nonreader controlled side, or —and in addition— to automatically unlock the door. Once the door switch is toggled, a DOOR HELD OPEN message is generated if the door is not closed within the time defined in the door switch point record.

Designed for high-traffic areas, this feature enhances the REX / Door switch functionality by providing a method to reset the door switch timer while the door is being held open. While employees continue to present valid keys and to pass through the door (causing the REX point to continually change state), the door switch timer is reset each time to the number of seconds in the door switch point record, thus preventing a DOOR HELD OPEN message from being generated. (The message *is* generated if the time between key presentation exceeds the time value in the record.)

---

This feature is enabled / disabled using the REXEXTEND parameter in the \$DATAPATH/NPOLLER.x file where x is the associated 708P poller number. The feature is enabled / disabled during installation, or may be changed as needed by the system administrator. If changed, the poller must be halted and restarted for the parameters to take effect. The recognized REXEXTEND values are:

Parameter missing — REXEXTEND defaults to 0 (feature disabled)  
 REXEXTEND=0 — Feature disabled  
 REXEXTEND=1 — Feature enabled

#### NOTE

The enable / disable condition as set applies to *all* devices controlled by the poller.

### KEY INVENTORY [invtmnu]

This feature is used to control system keys. This is an optional feature and does not effect operation. The menu screen is accessed from the main menu:

```
[invtmnu]      Key Inventory Menu
                Inventory Status Code Menu
                Key Inventory Entry
                Key Inventory Report
                Enter Selection:
```

### INVENTORY STATUS CODE MENU [statentr]

Key codes and descriptions are selected by the user (Code 1=*Key in use* is frequently set). Other code descriptions could be: *Key available*, *Key damaged*, *Key issued*, *Key lost*, *Key reported stolen*. In most cases, from four to ten (maximum) are set. The key codes and descriptions are entered using the key inventory status code entry screen:

```
[statentr]    Inventory Status Code Entry
                Inventory Code      : 1
                Inventory Description: AVAILABLE
```

### KEY INVENTORY STATUS CODE REPORT [statrprt]

This report lists established key codes (for a current key status report, see *Key Inventory Report* (following subsection)). A sample screen and report follow:

```
[statrprt] Inventory Status Code Report
Ready to produce Report. OK to continue? (Y/N)(Y) █
```

```
03/25/96 Ataraxia Electronics Page 1
15:52 Inventory Status Code Report
```

| Code | Code Description |
|------|------------------|
| 1    | AVAILABLE        |
| 2    | ASSIGNED         |
| 3    | LOST             |
| 4    | UNUSABLE         |
| 5    | DAMAGED          |
| 6    | TERMINATED       |
| 7    | REISSUED         |
| 8    | RECOVERED        |
| 9    | PREVIOUS OWNER   |
| 10   | RESERVED         |

### KEY INVENTORY ENTRY [cdinentr]

This function is used to add/change key inventory information (to delete a key record, use the system delete record feature — Esc, d, r):

```
[cdinentr] Key Inventory Entry
Key Type : 1 Facility Code : 0034 Key #: 30463
Keyholder ID: 7 Lastname: RUSS Firstname: ANDY
Tenant : 0 = BUILDING ADMINISTRATION
Status : 2 = ASSIGNED
Date : 05/08/92
Time : 15:16
Remarks :
```

### KEY INVENTORY REPORT [cdinrprt]

A sample screen and report follow:

```
[cdinrprt] Key Inventory Report
Lower Limit Upper Limit
Key Number : 3
Keyholder ID :
Tenant Number:

Sort Sequence: 1) Name, Keyholder ID
                2) Keyholder ID
```

| 03/25/96<br>15:55 |                   | Alpha Systems<br>Key Inventory Report |          |       | Page 1         |         |
|-------------------|-------------------|---------------------------------------|----------|-------|----------------|---------|
| Keyholder         | Keyholder Name    | Key No                                | Date     | Time  | Status Descrip | Remarks |
| 29205             | THORPE JAMES      | 29606                                 | 06/23/96 | 13:15 | ASSIGNED       |         |
| 31408             | ROSS MICHAEL      | 31409                                 | 06/23/96 | 13:22 | ASSIGNED       |         |
| 33244             | DESJARDINS ROBERT | 33249                                 | 06/23/96 | 13:25 | ASSIGNED       |         |
| 36427             | JERRY TIMOTHY     | 36426                                 | 06/23/96 | 13:44 | ASSIGNED       |         |
| 37441             | JUDD AL           | 37444                                 | 06/23/96 | 13:51 | ASSIGNED       |         |

## PARKING STICKERS [stkrmenu]

This feature is used to control parking stickers issued to keyholders. The initial screen is accessed from the main menu:

```

[stkrmenu]      Parking Sticker Menu

Parking Sticker Entry
Parking Sticker Interactive Display
Parking Sticker Master Report

Enter Selection:
  
```

## PARKING STICKER ENTRY [stkrentr]

```

[stkrentr]      Parking Sticker Entry

Keyholder ID: [REDACTED]      Key Number:
First Name :                  Last Name :
  
```

Enter the required information; the second parking entry screen automatically displays:

```

[stklentr]      Sticker Number and License Plate Entry

Sticker Number      License Plate
[REDACTED]
  
```

## PARKING STICKER INTERACTIVE DISPLAY [stkrprt1]

This function is used to determine keyholder location. Enter the keyholder ID; the location data displays automatically:

```

[stkrprt1]      Parking Sticker Interactive Display

                  Keyholder ID: 300066109

Last Name: TIM                First Name: D+NP                Visitor: M
Company   : 3      = WESTINGHOUSE SECURITY ELEC.
Dept     : 3      = ENGINEERING
Location : 2      = SANTA CLARA, CA - TECHMART BLD
Phone    : 408 727-5170

```

## PARKING STICKER MASTER REPORT [stkrprt]

The report lists assigned parking stickers. A sample screen and report follow:

```

[stkrprt]      Parking Sticker Master Report

Sort Sequence: 2

(1=Keyholder ID; 2=last Name; 3=Sticker Number)

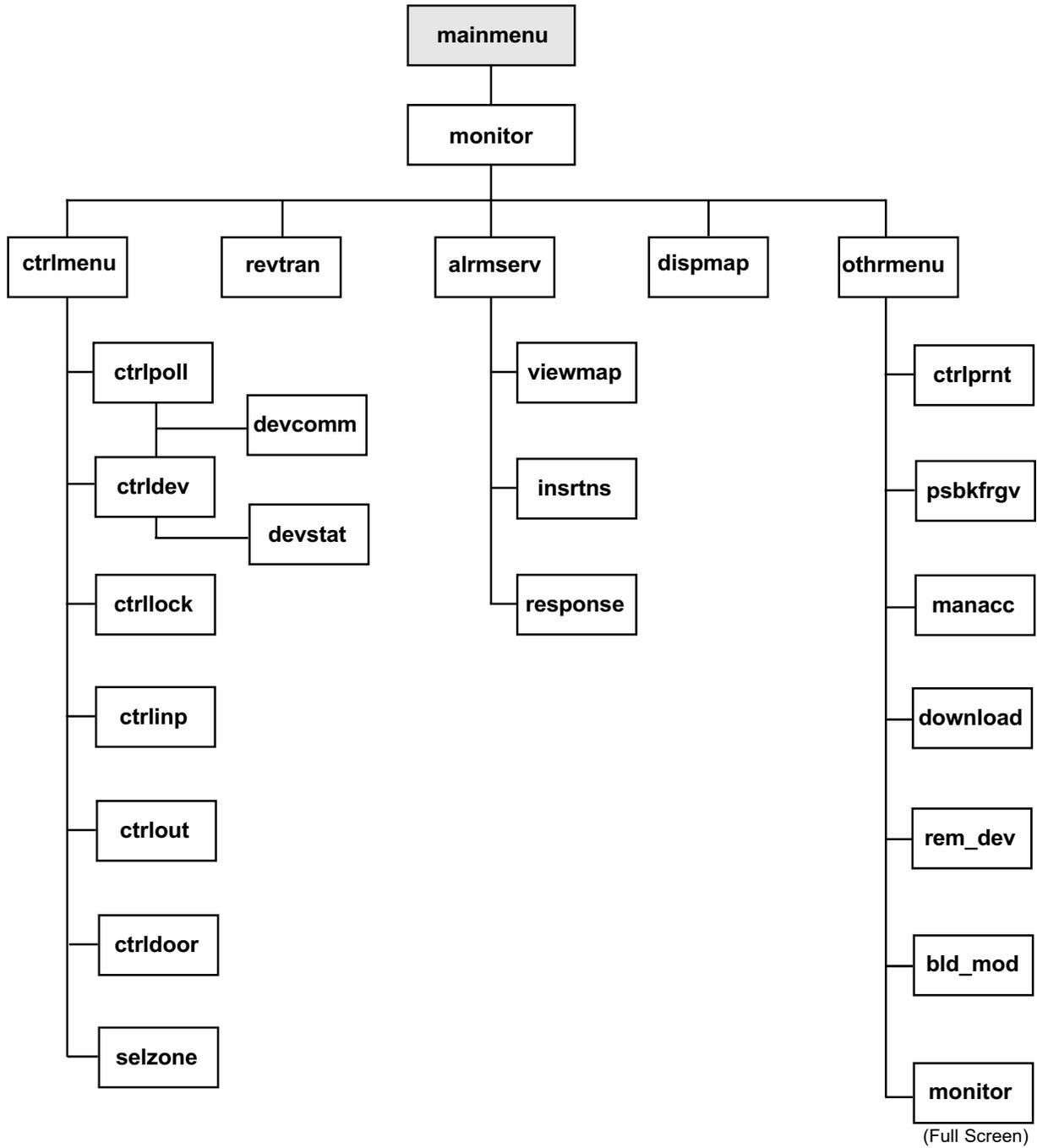
```

```

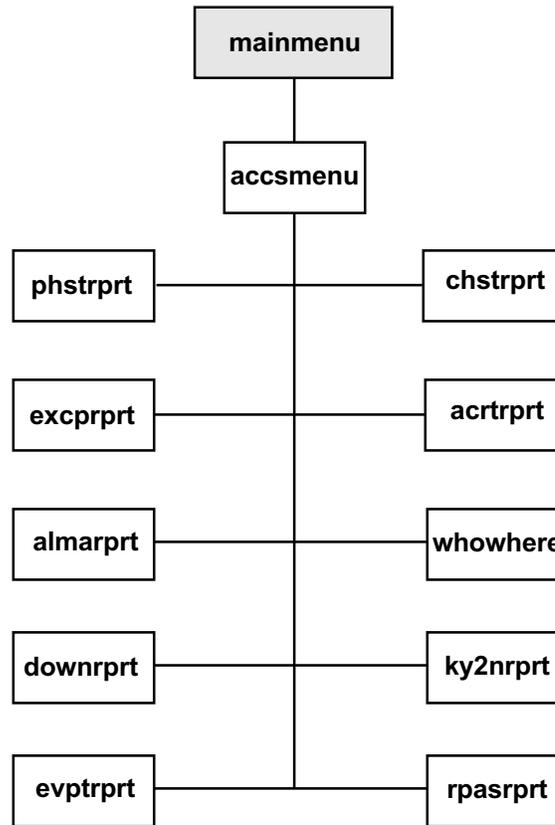
06/25/96                Security Electronics                Page 1
16:00                   Parking Sticker Report

```

| Keyholder | Keyholder Name   | Sticker | License |
|-----------|------------------|---------|---------|
| 28870     | TERRY VALE       | 500003  | 2MJK239 |
| 28977     | JESS WHITTINGTON | 500031  | 4B03048 |
| 28993     | CHERYL ROBERTS   | 500032  | 4888308 |
| 29001     | PETER VAUGHAN    | 500001  | 2PQS707 |

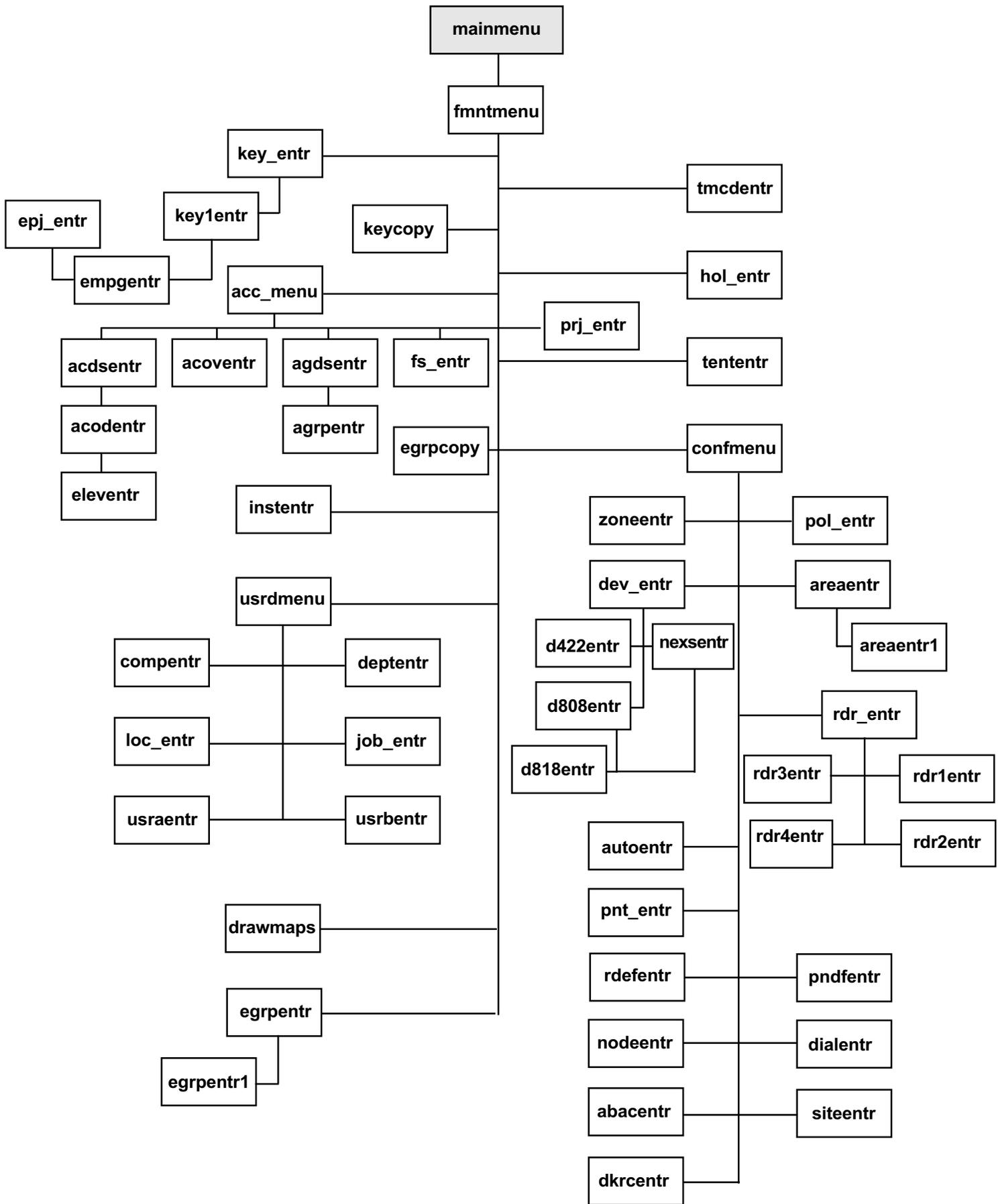


Screen Location Tree — Monitor Security Activity

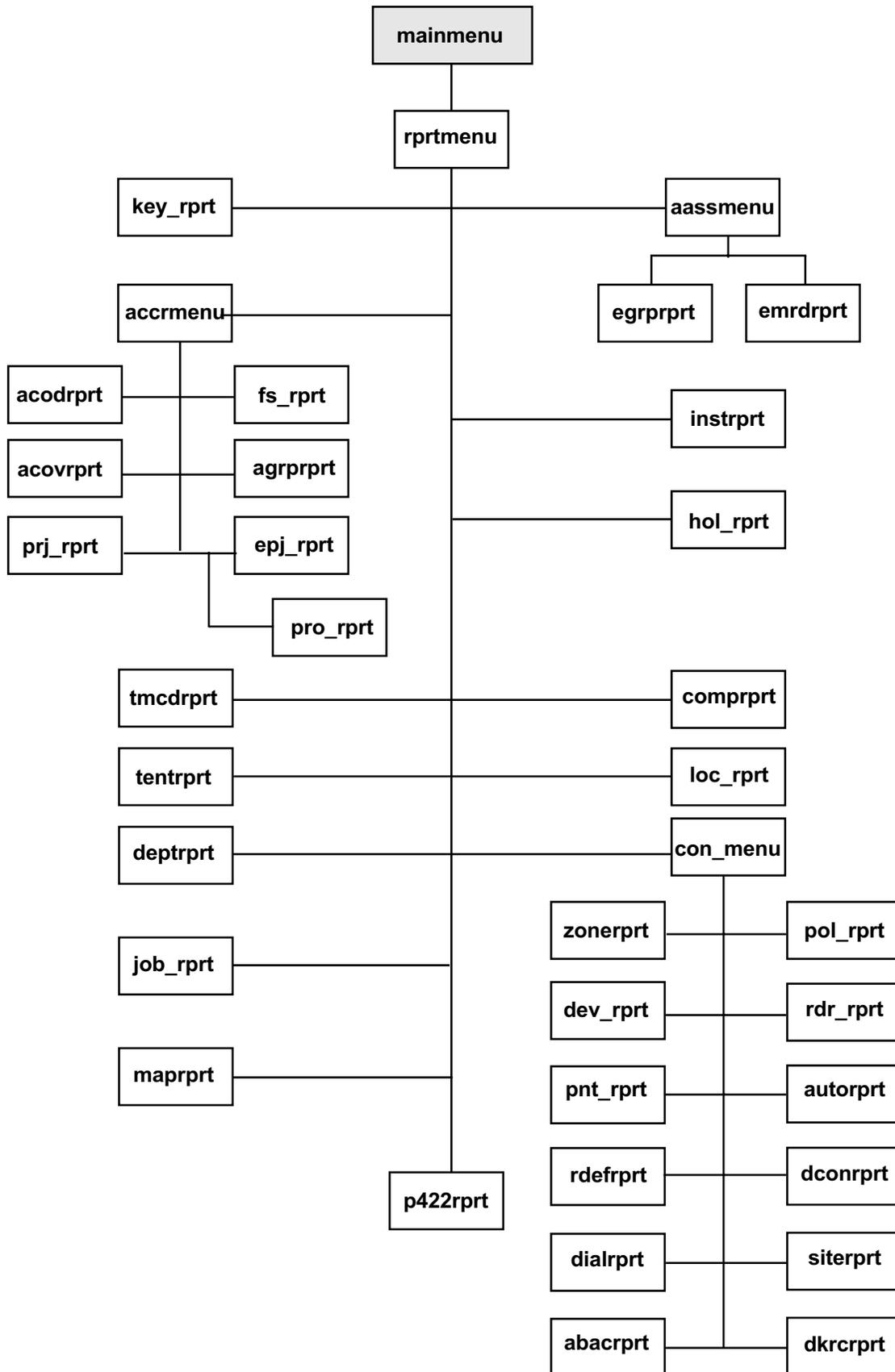


Screen Location Tree — Security Management Reports

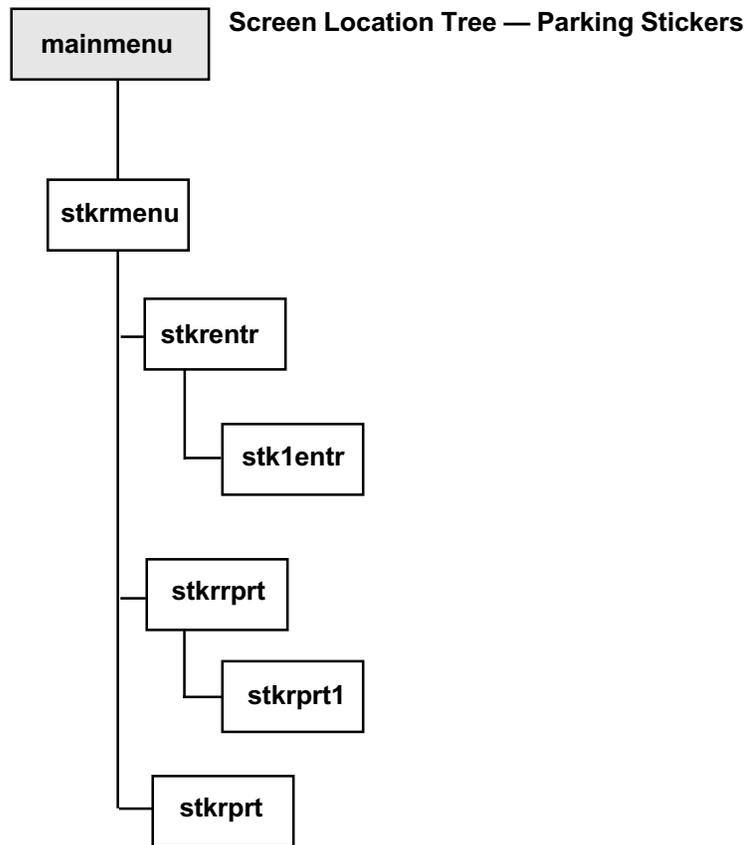
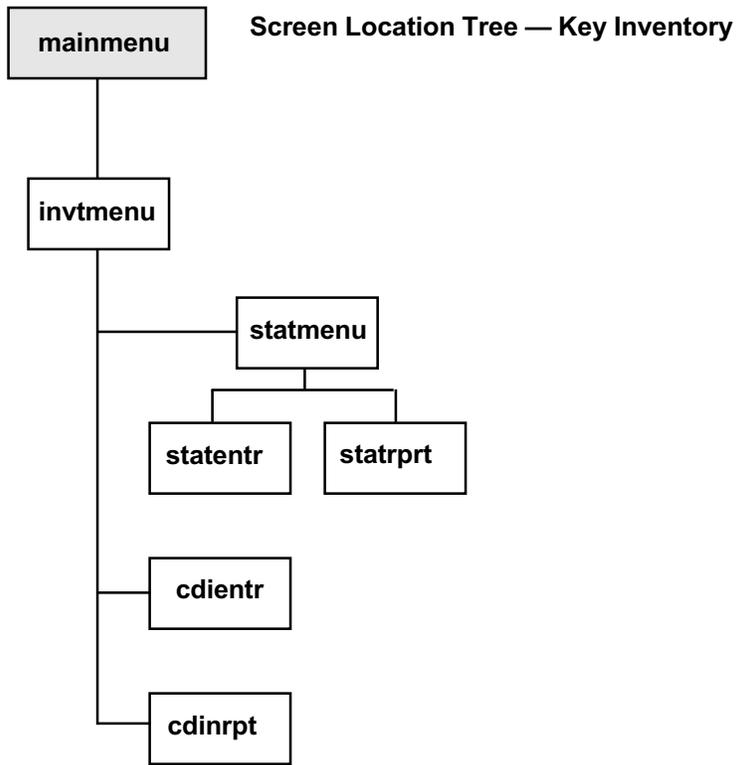
---

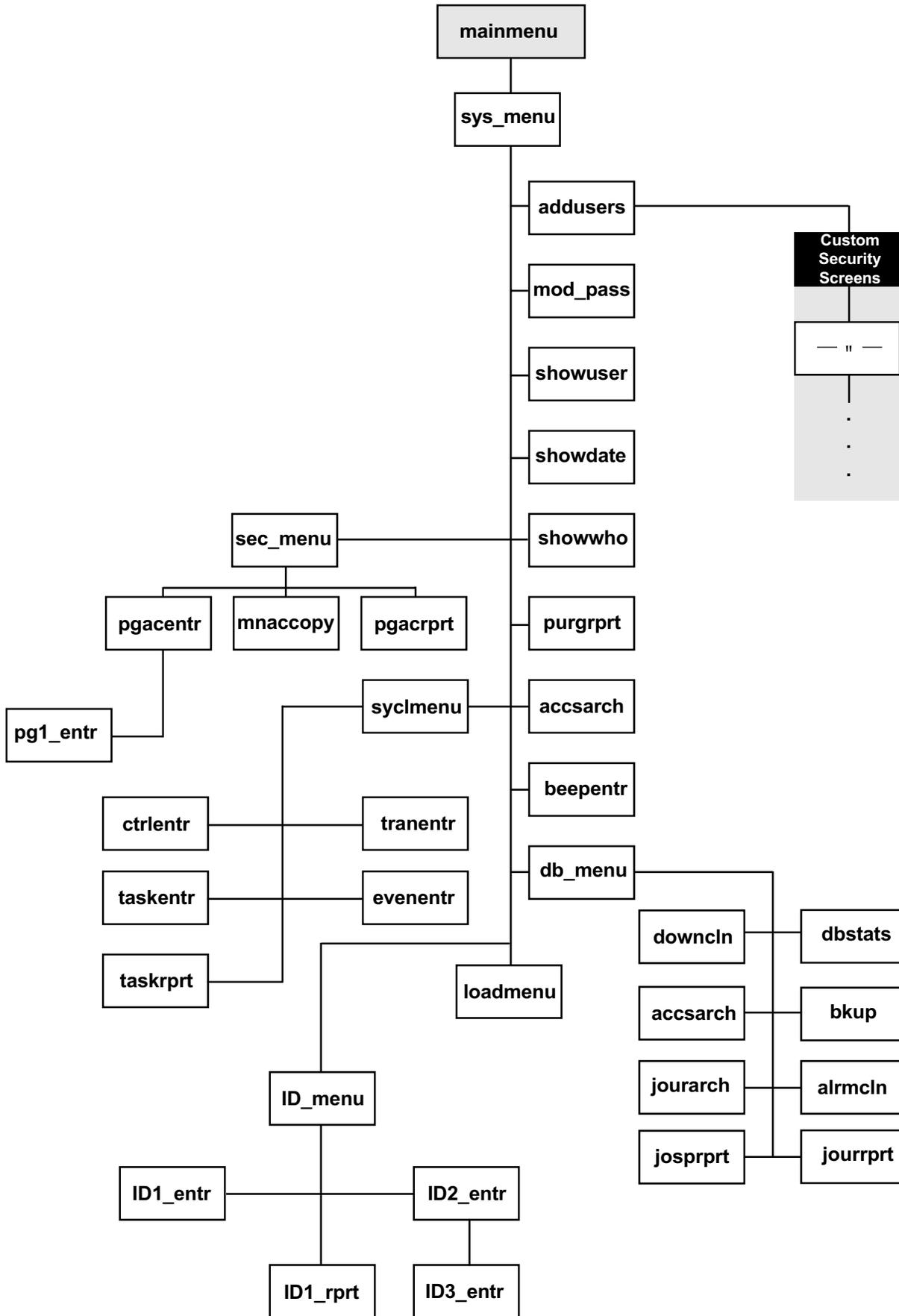


Screen Location Tree — Master File Entry



Screen Location Tree — Master File Reports





Screen Location Tree — System Administration

**MONITOR SECURITY ACTIVITY**

| SCREEN TITLE    | FUNCTION   |
|-----------------|--|
| <b>monitor</b>  | Watch events and activities as they occur; menu to other monitoring and control screens.   |
| <b>ctrlmenu</b> | Menu to control functions. Zone selection stays in effect until this screen is exited.     |
| <b>ctrlpoll</b> | Select pollers to halt or restart, and to check device communication.                      |
| <b>devcomm</b>  | Check communication between computer and attached devices.                                 |
| <b>ctrldev</b>  | Select devices to reset / shunt / unshunt, and to check status.                            |
| <b>devstat</b>  | Check point status for a particular device.  |
| <b>ctrllock</b> | Select locks to open, lock, time open, shunt, unshunt.                                     |
| <b>ctrlinp</b>  | Select input points to shunt, unshunt.   |
| <b>ctrlout</b>  | Select output points to activate, deactivate, shunt, unshunt.                              |
| <b>ctrldoor</b> | Select door switch points to view status, shunt, unshunt.                                  |
| <b>selzone</b>  | Select zone to which the control and monitoring will be limited.                           |
| <b>revtran</b>  | Page forwards / backwards through the last 5,000 system transactions.                      |
| <b>alrmserv</b> | Display currently pending alarms; provides response instructions, map.                     |
| <b>viewmap</b>  | Display user-created map showing alarm locations.  |
| <b>insrtns</b>  | Display user-created list of actions to be taken when an alarm occurs at a specific point. |
| <b>response</b> | View copy of alarm instructions; enter actions taken in response to the alarm.             |
| <b>dispmap</b>  | Display user-created system maps showing alarms, door status, lock status, etc.            |
| <b>othrmenu</b> | Menu to several system control functions.  |
| <b>ctrlprnt</b> | Reset, turn on, turn off system log printers.  |
| <b>psbkfrgv</b> | Restore passback status for a single keyholder, or for all keyholders in the system.       |
| <b>manacc</b>   | Allow entry for keyholder who does not have a key (operator and keyholder data logged).    |
| <b>download</b> | Extract database information, then update memory for host and attached devices.            |
| <b>rem_dev</b>  | Establish connection with a remotely connected device.                                     |
| <b>bld_mod</b>  | View and control building modes for individual ACUs or all ACUs in a zone.                 |
| <b>monitor</b>  | Provides a full-screen display (22 lines) of real-time transactions.                       |

**SECURITY MANAGEMENT REPORTS**

| SCREEN TITLE    | FUNCTION   |
|-----------------|--|
| <b>accsmenu</b> | Menu to the security management reporting functions.   |
| <b>phstrprt</b> | Report last twenty activities which took place at a specific point.  |
| <b>chstrprt</b> | Report last twenty activities which took place for a specific keyholder.   |
| <b>excprprt</b> | Report transactions currently stored on the hard disk.   |
| <b>acrtrprt</b> | Report transactions currently stored on tape.  |
| <b>almarprt</b> | Report of operator responses to alarms.  |
| <b>whowhere</b> | Report number of keyholders in each passback level.  |
| <b>downrprt</b> | Report database changes. Serves also as an audit trail of operator activity.   |
| <b>k2nrprt</b>  | Report last zone entered (summary or detail). Uses keyholder history as source.  |
| <b>evptrprt</b> | Report system events — totals for each event within a selected date range.   |
| <b>rpasrprt</b> | Report real-time zone passback activity showing how many and / or who is currently in which zone. Uses shared memory data as source. |

**MASTER FILE ENTRY**

| SCREEN TITLE    | FUNCTION  |
|-----------------|---|
| <b>key_entr</b> | Enter primary keyholder information: keyholder ID, key number, name, tenant, etc. |
| <b>key1entr</b> | Enter keyholder personal information: address, phone, title, floor, remarks, etc. |
| <b>empgentr</b> | Assign access privileges to a keyholder.  |
| <b>epj_entr</b> | Assign projects to a keyholder.   |

---

|                  |  |
|------------------|--|
| <b>key_copy</b>  | Create new keyholder record by copying from an existing keyholder record.                  |
| <b>egrpentr</b>  | Select a keyholder for access privilege assignment. Can also be reached from key1entr.     |
| <b>egrpentr1</b> | Assign access privileges to a keyholder.   |
| <b>egrpcopy</b>  | Copy one keyholder's information to another keyholder.                                     |
| <b>acc_menu</b>  | Menu to reach the access definition functions.   |
| <b>acdsentr</b>  | Enter / modify access code information.  |
| <b>acodentr</b>  | Add key readers to an access code.   |
| <b>eleventr</b>  | Enter elevator output contact information for a specific reader in a specific access code. |
| <b>acoventr</b>  | Temporarily override keyholder or keyholder group access.                                  |
| <b>agdsentr</b>  | Enter / modify access groups.  |
| <b>agrpentr</b>  | Add access codes to an access group.   |
| <b>fs_entr</b>   | Enter / modify fail-soft access capabilities for a 708P.                                   |
| <b>prj_entr</b>  | Define projects, start / stop dates and times.   |
| <b>tmcdentr</b>  | Enter / modify time code information.  |
| <b>hol_entr</b>  | Enter / modify holiday information.  |
| <b>tententr</b>  | Enter / modify tenant information.   |
| <b>instentr</b>  | Enter / modify alarm point information   |
| <b>confmenu</b>  | Menu to the system configuration functions.  |
| <b>zoneentr</b>  | Enter / modify zone information.   |
| <b>areaentr</b>  | Enter / modify areas.  |
| <b>areaentr1</b> | Enter / modify zones in areas.   |
| <b>pol_entr</b>  | Enter / modify poller information.   |
| <b>dev_entr</b>  | Enter / modify device information .  |
| <b>nexsentr</b>  | Enter / modify information specific to NexSentry.  |
| <b>d808entr</b>  | Enter / modify information specific to 808S.   |
| <b>d818entr</b>  | Enter / modify information specific to 818x.   |
| <b>d422entr</b>  | Enter / modify information specific to SE 422.   |
| <b>rdr_entr</b>  | Enter / modify reader / key pad information.   |
| <b>rdr1entr</b>  | Enter / modify reader information specific to 808S.  |
| <b>rdr2entr</b>  | Enter / modify reader information specific to SE 422.                                      |
| <b>rdr3entr</b>  | Enter / modify reader information specific to 818x.  |
| <b>rdr4entr</b>  | Enter / modify reader information specific to NexSentry.                                   |
| <b>pnt_entr</b>  | Enter / modify point information.  |
| <b>autoentr</b>  | Enter auto-activation / auto-opening times for points / readers.                           |
| <b>rdefentr</b>  | Define 808S action reports.  |
| <b>pndfentr</b>  | Define default number of digits and seed the PIN (SE 422).                                 |
| <b>nodeentr</b>  | Enter / modify sub-device information for SE 422.  |
| <b>dialentr</b>  | Enter / modify remotely connected device information.                                      |
| <b>siteentr</b>  | Define site configuration for SE 422.  |
| <b>abacentr</b>  | Define ABA (magnetic stripe card) configuration.   |
| <b>dkrcentr</b>  | Define digital key reader configuration.   |
| <b>usrdmenu</b>  | Menu to the user-defined field entry screens.  |
| <b>compentr</b>  | Enter / modify user-defined field A (appears on key_entr).                                 |
| <b>deptentr</b>  | Enter / modify user-defined field B (appears on key_entr).                                 |
| <b>loc_entr</b>  | Enter / modify user-defined field C (appears on key_entr).                                 |
| <b>job_entr</b>  | Enter / modify user-defined field D (appears on key_entr).                                 |
| <b>usraentr</b>  | Enter / modify user-defined field E (appears on key_entr).                                 |
| <b>usrbentr</b>  | Enter / modify user-defined field F (appears on key_entr).                                 |
| <b>drawmaps</b>  | Create real-time control maps / alarm location maps.                                       |

**MASTER FILE REPORTS**

| <b>SCREEN TITLE</b> | <b>FUNCTION</b>   |
|---------------------|---|
| <b>rprtmenu</b>     | Menu to database reporting functions.                           |
| <b>key_rprt</b>     | Report keyholder information.                                   |
| <b>aassmenu</b>     | Menu to the access assignment reporting functions.              |
| <b>egrprprt</b>     | Report access codes / access groups assigned to keyholders.     |
| <b>emrdrprt</b>     | Report specific readers assigned to keyholders.                 |
| <b>accrmenu</b>     | Menu to the access definition reporting functions.              |
| <b>acodrprt</b>     | Report readers and time codes for the access codes.             |
| <b>agrprprt</b>     | Report access assignments for access groups.                    |
| <b>acovrprt</b>     | Report access override data.                                    |
| <b>fs_rprt</b>      | Report fail-soft access privileges for 708P.                    |
| <b>prj_rprt</b>     | Report all projects.  |
| <b>epj_rprt</b>     | Report all keyholders assigned to projects.                     |
| <b>pro_rprt</b>     | Report all projects / readers included in individual projects.  |
| <b>tmcdrprt</b>     | Report all time codes.  |
| <b>hol_rprt</b>     | Report all defined holidays.                                    |
| <b>tentrprt</b>     | Report all defined tenants.                                     |
| <b>comprprt</b>     | Report all user-defined field A information.                    |
| <b>deprprt</b>      | Report all user-defined field B information.                    |
| <b>loc_rprt</b>     | Report all user-defined field C information.                    |
| <b>job_rprt</b>     | Report all user-defined field D information.                    |
| <b>instrprt</b>     | Report all alarm instructions.                                  |
| <b>map_rprt</b>     | Report all map names for specific point IDs.                    |
| <b>con_menu</b>     | Menu to the system configuration reporting functions.           |
| <b>zonerprt</b>     | Report all defined zones.                                       |
| <b>pol_rprt</b>     | Report all defined pollers.                                     |
| <b>dev_rprt</b>     | Report all defined device information.                          |
| <b>rdr_rprt</b>     | Report all defined readers.                                     |
| <b>pnt_rprt</b>     | Report all point information                                    |
| <b>autorprt</b>     | Report all point / reader auto-activate / auto-open information |
| <b>rdefrprt</b>     | Report all defined 808S action report information.              |
| <b>dconrprt</b>     | Report all remotely connected devices.                          |
| <b>dialrprt</b>     | Report all remote site information.                             |
| <b>siterprt</b>     | Report all defined ABA sites                                    |
| <b>abacrprt</b>     | Report all defined ABA configurations.                          |
| <b>dkrcrprt</b>     | Report all digital key reader information.                      |
| <b>p422rprt</b>     | Report all keyholders for SE 422 (detailed or summary).         |

**KEY INVENTORY**

| <b>SCREEN TITLE</b> | <b>FUNCTION</b>                            |
|---------------------|--|
| <b>invrtmenu</b>    | Menu to key Inventory functions.           |
| <b>statmenu</b>     | Menu to the status definition functions.   |
| <b>statentr</b>     | Enter key inventory status codes.          |
| <b>statrprt</b>     | Report all inventory status codes.         |
| <b>cdinentr</b>     | Enter key data.                            |
| <b>cdinrprt</b>     | Report inventory information for all keys. |

---

**PARKING STICKERS**

| SCREEN TITLE    | FUNCTION   |
|-----------------|--|
| <b>stkrmenu</b> | Menu to parking sticker and license plate management functions.                    |
| <b>stkrentr</b> | Select keyholder for parking sticker and / or license plate information entry.     |
| <b>stk1entr</b> | Enter parking sticker or license plate information for keyholder.                  |
| <b>stkrprt</b>  | Locate keyholder by license plate or parking sticker.                              |
| <b>stkrprt1</b> | Display keyholder location information by license plate or parking sticker number. |
| <b>stkrprt</b>  | Report all parking sticker / license plate information.                            |

**SYSTEM ADMINISTRATION**

| SCREEN TITLE     | FUNCTION  |
|------------------|---|
| <b>sys_menu</b>  | Menu to the system administration functions.  |
| <b>addusers</b>  | Add operator to system.   |
| <b>mod_pass</b>  | Change operator passwords.  |
| <b>sec_menu</b>  | Menu to the security level definition functions.  |
| <b>pgacentr</b>  | Create / modify security levels.  |
| <b>pg1_entr</b>  | Add / modify screen information for a particular security level.                          |
| <b>mnacopy</b>   | Create new security level by copying existing security level then modifying.              |
| <b>pgacrprt</b>  | Report all defined security levels.   |
| <b>showuser</b>  | Display all system operators.   |
| <b>showdate</b>  | Display current system date and time.   |
| <b>showwho</b>   | Display operators currently using the system.   |
| <b>purgrrprt</b> | Cancel submitted reports.   |
| <b>beepentr</b>  | Define terminals for alarm response (beep) regardless of system area where operating.     |
| <b>syclmenu</b>  | Menu to system configuration functions  |
| <b>ctrlentr</b>  | Change report titles / user-defined fields. Define terminal for automatic alarm response. |
| <b>evenentr</b>  | Enter / modify event information.   |
| <b>taskentr</b>  | Enter / modify task information.  |
| <b>taskrprt</b>  | Report all tasks / events.  |
| <b>tranentr</b>  | Enter / modify transaction information (controls data display and storage).               |
| <b>dbmenu</b>    | Menu to the database administration functions.  |
| <b>dbstats</b>   | Display size of database tables (determines if archiving is required).                    |
| <b>bkup</b>      | Backup database to tape.  |
| <b>downcln</b>   | Remove unwanted records from the download file.   |
| <b>accsarch</b>  | Transfer records from disk to tape to free up disk space.                                 |
| <b>almcln</b>    | Remove operator responses to alarms from disk to free up disk space.                      |
| <b>jourarch</b>  | Copy journal records to tape and remove from disk.  |
| <b>jourrprt</b>  | Report history of all database changes.   |
| <b>josrprt</b>   | Report history of all changes to keyholder and keyholder access assignment information.   |
| <b>loadmenu</b>  | Load keyholder information from ASCII files.  |
| <b>ID_menu</b>   | ID security maintenance menu for WSE ID-4000 interface option.                            |
| <b>ID1_entr</b>  | Enter users, passwords, and privileges for WSE ID-4000 operators.                         |
| <b>ID2_entr</b>  | Define security groups for WSE ID-4000 operators.   |
| <b>ID3_entr</b>  | Define specific operator privileges for a security group.                                 |

---

| #  | Message                       | Explanation  |
|----|-------------------------------|--|
| 0  | <b>Negative Acknowledge</b>   | 708P unable to understand message from host.                     |
| 1  | <b>Access Granted</b>         | Card or keypad entry granted access by ACU or host.              |
| 2  | <b>Key Trace</b>              | Card flagged as TRACE has been read.                             |
| 3  | <b>Point Trace</b>            | A card has been read by a sensor flagged as TRACE.               |
| 4  | <b>Invalid Time</b>           | Access denied — card not valid at that time.                     |
| 5  | <b>Invalid Day</b>            | Access denied — card not valid that day.                         |
| 6  | <b>Invalid Reader</b>         | Access denied — card not valid at that sensor.                   |
| 7  | <b>Key Not Active Yet</b>     | Access denied — card presented prior to issue date.              |
| 8  | <b>Key Terminated</b>         | Access denied — card presented after return date.                |
| 9  | <b>Point Disabled</b>         | Access denied — sensor disabled.                                 |
| 10 | <b>Point Not On File</b>      | Sensor or point not defined in the host computer.                |
| 11 | <b>Key Not On File</b>        | Access denied — key not in ACU or host memory.                   |
| 12 | <b>Invalid Facility Code</b>  | Access denied — wrong facility code (1030/1040 keys only).       |
| 13 | <b>Manual Unlock</b>          | Reader / door manually unlocked.                                 |
| 14 | <b>Manual Lock</b>            | Reader / door manually locked.                                   |
| 15 | <b>Auto Unlock</b>            | Reader / door auto-unlocked by host or ACU.                      |
| 16 | <b>Auto Lock</b>              | Reader / door auto-locked by host or ACU.                        |
| 17 | <b>Door Forced Open</b>       | Door with status switch opened without card or REX.              |
| 18 | <b>Door Held Open</b>         | Door with status switch remains open beyond set time.            |
| 19 | <b>Door Closed (Forced)</b>   | Forced door has now been closed.                                 |
| 20 | <b>Door Closed (Held)</b>     | Door held open too long has now been closed.                     |
| 21 | <b>Access Requested</b>       | Valid key presented; host waiting for corresponding keypad entry |
| 22 | <b>Poller Died</b>            | Software poller has failed.                                      |
| 23 | <b>Poller Can't Open Port</b> | Hardware poller has failed (poller device open error).           |
| 24 | <b>Poller Started</b>         | Poller started.  |
| 25 | <b>Poller Stopped</b>         | Poller stopped.  |
| 26 | <b>Host Comm. Started</b>     | Communication initiated between host and LC / RLC.               |
| 27 | <b>Host Comm. Stopped</b>     | Communication ended between host and LC / RLC.                   |
| 28 | <b>Printer Off</b>            | Log printer switched off.  |

| #  | Message                       | Explanation  |
|----|-------------------------------|--|
| 29 | <b>Printer On</b>             | Log printer switched on.   |
| 30 | <b>Device Reset</b>           | 708P / 8xx-series powered up / re-initialized.   |
| 31 | <b>Return From Failsoft</b>   | 708P communication restored — no longer in failsoft mode.                                |
| 32 | <b>Power Failed</b>           | 708P / 8xx-series with 3708 UPS has lost AC power.                                       |
| 33 | <b>Power Restored</b>         | 708P / 8xx-series with 3708 UPS has regained AC power.                                   |
| 34 | <b>Tamper Active</b>          | 708P / 8xx-series tamper input active.   |
| 35 | <b>Tamper Clear</b>           | 708P / 8xx-series active tamper input now cleared.                                       |
| 36 | <b>COAX Failure</b>           | Coax cable from ACU to reader shorted.   |
| 37 | <b>COAX OK</b>                | Coax cable from ACU to reader repaired.  |
| 38 | <b>Sensor Failure</b>         | ACU has lost communication with reader (open coax).                                      |
| 39 | <b>Sensor OK</b>              | Previously failed reader (or open coax) repaired.  |
| 40 | <b>Printer Error</b>          | Log printer is not functioning properly.   |
| 41 | <b>Poller Params Reloaded</b> | Host has initialized a poller.   |
| 42 | <b>Still Held Open</b>        | DOOR HELD OPEN — Second alert message.   |
| 43 | <b>Input Point Active</b>     | A GENERAL input has been activated.  |
| 44 | <b>Input Point Normal</b>     | Previously activated GENERAL input point has been cleared.                               |
| 45 | <b>Timeout Device</b>         | Response from polled ACU by host not received within allotted time (usually 2 seconds).  |
| 46 | <b>Unable to Lock Door</b>    | Host unable to implement automatic or manual command to lock a door (error on lock).     |
| 47 | <b>Unable to Unlock Door</b>  | Host unable to implement automatic or manual command to unlock a door (error on unlock). |
| 48 | <b>Unable to Clear Output</b> | Host unable to restore output contact to normal (error on output clear).                 |
| 49 | <b>Unable to Act. Output</b>  | Host unable to restore output contact to active (error on output clear).                 |
| 50 | <b>Not Used</b>               | Reserved for future applications.  |
| 51 | <b>Not Used</b>               | Reserved for future applications.  |
| 52 | <b>Manual Unlock Timed</b>    | Timed unlock command entered.  |
| 53 | <b>Manual Access Granted</b>  | Manual access command issued.  |

| #  | Message                         | Explanation   |
|----|---------------------------------|---|
| 54 | <b>Device Online</b>            | ACU communicating with host.  |
| 55 | <b>Request Manual Access</b>    | Manual access command entered.  |
| 56 | (Building Closed Trace)         | Obsolete message  |
| 58 | <b>Repack OK</b>                | Host has loaded new database information.   |
| 59 | <b>Error Setting Bldg. Mode</b> | Building mode command unsuccessful.   |
| 60 | <b>Key Activated</b>            | Key presented to activate reader — activate card enabled.                                   |
| 61 | <b>Key Deactivated</b>          | Key presented to deactivate reader — deactivate card enabled.                               |
| 62 | <b>Key Not Active</b>           | Access denied — key applies to activate reader.   |
| 63 | <b>New Day</b>                  | Host rebooted or clock has crossed 00:00.   |
| 64 | <b>Remote Trans Received</b>    | Dial-up device transmission received by host.   |
| 65 | <b>Host Dial OK</b>             | Host has called a dial-up device.   |
| 66 | <b>Error Dialing Remote</b>     | Download errors to remote dial-up device encountered.                                       |
| 67 | <b>Output Activated</b>         | Output contact manually or automatically activated.   |
| 68 | <b>Output Deactivated</b>       | Output contact manually or automatically deactivated.                                       |
| 69 | <b>Invalid PIN Entered</b>      | PIN entered incorrect.  |
| 70 | <b>Redundancy On</b>            | Not used at this time.  |
| 71 | <b>Redundancy Off</b>           | Not used at this time.  |
| 72 | <b>Host Poller Down</b>         | Not used at this time.  |
| 73 | <b>Acknowledge DB Xfer</b>      | Data successfully downloaded to target device.  |
| 74 | <b>Failed DB Xfer</b>           | Data download attempt to target device failed.  |
| 75 | <b>No Key Set for PIN</b>       | PIN entered without valid key presentation.   |
| 76 | <b>Keyholder Duress</b>         | PIN entered in reverse sequence indicating a duress situation. If valid, access is granted. |
| 77 | <b>Controller Comm Error</b>    | Host to local controller communication failed.  |
| 78 | <b>RDI Dialed In</b>            | RDI unit has dialed host and is logged in.  |
| 79 | <b>Lot Full</b>                 | Optional parking function.  |
| 80 | <b>Max Tenant In Lot</b>        | Optional parking function.  |
| 81 | <b>Alarm Resolved</b>           | Alarm event resolved.   |
| 82 | <b>Enter Attended Mode</b>      | Optional parking function.  |

| #   | Message                       | Explanation   |
|-----|-------------------------------|---|
| 83  | <b>Enter Unattended Mode</b>  | Optional parking function.  |
| 84  | <b>Batch Request Received</b> | Not used at this time.  |
| 85  | <b>Remote Comm Ended</b>      | Not used at this time.  |
| 86  | <b>Global Silence Request</b> | Silence global beeping command issued.                              |
| 89  | <b>Ticket Serviced</b>        | Parking application has completed ticket update/storage activities. |
| 90  | <b>Chksum Err In Sys DB</b>   | Difference exists between host and ACU system data.                 |
| 91  | <b>Chksum Err In Key DB</b>   | Difference exists between host and ACU key data.                    |
| 92  | <b>Alarm Active</b>           | Alarm input active.   |
| 93  | <b>Alarm Clear</b>            | Previously active alarm input cleared.                              |
| 94  | <b>Shunt Point</b>            | Device / point shunt command issued.                                |
| 95  | <b>Unshunt Point</b>          | Device / point unshunt command issued.                              |
| 96  | <b>Not Used</b>               | Reserved for future applications.                                   |
| 97  | <b>Parameter Load Error</b>   | Host poller initialization failed.                                  |
| 98  | <b>Tran File Almost Full</b>  | Archive history file approaching capacity. Archive immediately.     |
| 99  | <b>Database Error</b>         | Data to database failed. There may be many possible causes.         |
| 100 | <b>Passback Violation</b>     | Access denied — passback status.                                    |
| 103 | <b>Building Open</b>          | 808-series — ACU in open mode.                                      |
| 104 | <b>Building Open Limited</b>  | 808-series — ACU in limited mode.                                   |
| 105 | <b>Building Closed</b>        | 808-series — ACU in closed mode.                                    |
| 106 | <b>Tamper Report Shunted</b>  | 8xx-series ACUs — device tamper report is shunted.                  |
| 107 | <b>Tamper Report Unshunt</b>  | 8xx-series ACUs — device tamper report is unshunted.                |
| 108 | <b>Request To Exit</b>        | REX contact activated during valid REX time.                        |
| 109 | <b>REX Denied</b>             | REX contact activated during invalid REX time.                      |
| 110 | <b>MSM Fail</b>               | MSM failed.   |
| 111 | <b>MSM Okay</b>               | Previously failed MSM repaired.                                     |
| 112 | <b>Door Report Shunted</b>    | Door forced report shunted.   |
| 113 | <b>Door Report Unshunted</b>  | Door forced report unshunted.                                       |
| 114 | <b>Power Report Shunted</b>   | Device power fail report shunted.                                   |

| #           | Message                            | Explanation  |
|-------------|------------------------------------|--|
| 115         | <b>Power Report Unshunted</b>      | Device power fail report unshunted.  |
| 116         | <b>COAX Report Shunted</b>         | Reader coax fail report shunted.   |
| 117         | <b>COAX Report Unshunted</b>       | Reader coax fail report unshunted.   |
| 118         | <b>Sensor Report Shunted</b>       | Sensor / reader fail report shunted.   |
| 119         | <b>Sensor Report Unshunted</b>     | Sensor / reader fail report unshunted.   |
| 120         | <b>MSM Report Shunted</b>          | 8xx-series ACU MSM fail report shunted.  |
| 121         | <b>MSM Report Unshunted</b>        | 8xx-series ACU MSM fail report unshunted.  |
| 122         | <b>Power Report Shunted</b>        | 8xx-series ACU MSM power fail report shunted.                                    |
| 123         | <b>Power Report Unshunted</b>      | 8xx-series ACU MSM power fail report unshunted.                                  |
| 124         | <b>Bldg Opened</b>                 | 8xx-series ACU MSM power fail report shunted.                                    |
| 125         | <b>Bldg Opened Limited</b>         | 8xx-series ACU placed in limited mode.   |
| 126         | <b>Bldg Closed</b>                 | 8xx-series ACU placed in closed mode.  |
| 127         | <b>Bldg Should be Closed</b>       | 8xx-series ACU in time period where it should be closed.                         |
| 128         | <b>Can't Close Bldg (Key)</b>      | 8xx-series ACU cannot be placed in closed mode because proper key not presented. |
| 129         | <b>Can't Close Bldg - User</b>     | 8xx-series ACU cannot be placed in closed mode because of user actions.          |
| 130         | <b>Terminal Buffer Full</b>        | 8xx-series host port log buffer at capacity.                                     |
| 131         | <b>Device Cannot Connect</b>       | 8xx-series ACU unable to communicate with host / dial-up interface.              |
| 132         | <b>Alarm Silenced</b>              | 8xx-series ACU silenced by a user connected through the ACU terminal port.       |
| 133         | <b>Forgive Passback</b>            | Passback status on card / card group set to unknown.                             |
| 134         | <b>Invalid T &amp; A Request</b>   | No longer used.  |
| 135         | <b>Time &amp; Attendance Clock</b> | Key presented at a valid time and attendance reader.                             |
| 136         | <b>Meal Counter - Excp.</b>        | Keyholder over meal limit.   |
| 137         | <b>Meal Counter - Valid</b>        | Key presented at valid meal counter reader.                                      |
| 138 and 139 |                                    | Reserved for future applications.  |
| 140         | <b>User Logged Into Term</b>       | User logged on to 8xx-series ACU via the terminal port.                          |
| 141         | <b>User Logged Off Term</b>        | User logged off an 8xx-series ACU via the terminal port.                         |

| #               | Message               | Explanation   |
|-----------------|-----------------------|---|
| 142             | Host Dial Start       | Remote device dialing host.                             |
| 143             | Carrier Off           | SE 422—Incoming phone line or host port has lost DTR.   |
| 144             | Carrier On            | SE 422 — Incoming phone line or host port DTR high.     |
| 145             | Logs Purged           | SE 422 — Log buffer purged.                             |
| 146             | Threshold Met         | SE 422 — Logs have met user-defined threshold.          |
| 147             | Deferred Key          | Key referred to host for access decisions.              |
| 148             | Auto Forgive          | Automatic forgive passback issued.                      |
| 149             | Zone Count Reset      | Count for a particular zone or all zones reset.         |
| 150             | Req. Passback Forgive | Forgive passback command issued.                        |
| 151             | Timer Started         | Not used at this time.                                  |
| 152             | Timer Cancelled       | Not used at this time.                                  |
| 153             | Timer Expired         | Not used at this time.                                  |
| 154             | Request Reset Device  | Operator initiated device reset from devices menu.      |
| 155             | Request Reset Keys    | Operator initiated key reset from devices menu.         |
| 156             | Reset Device Okay     | Affirmative response following device reset command.    |
| 157             | Reset Key Okay        | Key information successfully reset in 8xx-series ACU.   |
| 158             | Error on Device Reset | Unable reset memory / system data for 8xx-series ACU.   |
| 159             | Error on Key Reset    | Unable reset key data for 8xx-series ACU.               |
| 160             | Open Cash Drawer      | Parking attendant cash drawer opened improperly.        |
| 161             | Invalid Card Type     | Wrong type magnetic stripe card presented.              |
| 162             | Line Cut              | SE 422 input line cut.                                  |
| 163             | Line Short            | SE 422 input line shorted.                              |
| 164 through 169 |                       | Reserved for future applications.                       |
| 170             | Over Device Limit     | System configuration has exceeded specified limits.     |
| 171             | Invalid Site Code     | Site code not on file or invalid.                       |
| 172             | ABA Card Expired      | ABA card presented has expired.                         |
| 173             | ABA Card Data 1       | Five 40-character lines (maximum) encoded on ABA cards. |
| 174             | ABA Card Data 2       | •   |
| 175             | ABA Card Data 3       | •   |
| 176             | ABA Card Data 4       | •   |
| 177             | ABA Card Data 5       | •   |

| #   | Message                   | Explanation  |
|-----|---------------------------|--|
| 178 | VIP Failure               | VIP keypad not responding.   |
| 179 | VIP Okay                  | VIP keypad returned from failed status.                                    |
| 180 | VIP Tamper Fail           | VIP tamper fail reported.  |
| 181 | VIP Tamper Okay           | VIP tamper switch OK.  |
| 182 | VIP Shunted               | VIP shunted.   |
| 183 | VIP Unshunted             | VIP unshunted.   |
| 184 | VIP Tamper Shunted        | VIP tamper switch shunted.   |
| 185 | VIP Tamper Unshunted      | VIP tamper switch unshunted.   |
| 200 | Radionics Unit Test       | For Radionics systems (for future use).                                    |
| 201 | General Trouble           | "  |
| 202 | Zone Trouble              | "  |
| 203 | Line Card Trouble         | "  |
| 204 | General Restoral Report   | "  |
| 205 | Zone Restoral             | "  |
| 206 | Line Card Restored        | "  |
| 207 | General Opening Report    | "  |
| 208 | Zone Opening Report       | "  |
| 209 | General Closing Report    | "  |
| 210 | Zone Closed               | "  |
| 211 | General Cancel Report     | "  |
| 212 | Zone Cancel Report        | "  |
| 213 | Radionics Unit Power Fail | "  |
| 214 | Radionics Unit Restore    | "  |
| 215 | Listen-In Report          | "  |
| 216 | Listen Done               | "  |
| 217 | Communicator Power Fail   | "  |
| 218 | Was Forced Armed          | "  |
| 219 | Status Report             | "  |
| 220 | Busy Seconds              | "  |
| 221 | Error                     | "  |
| 222 | Power Up Message          | "  |
| 223 | Radionics Alarm           | "  |
| 230 | Project Activated         | Project activated.   |
| 231 | Project Deactivated       | Active project deactivated.  |
| 232 | Project Normalized        | Project normalized.  |
| 233 | Invalid Project           | Access denied to a project-controlled door (no access privileges).         |
| 240 | Alarm Not Acknowledged    | No alarm response within time specified in transaction description record. |
| 241 | Alarm Acknowledged        | Alarm acknowledged.  |

| #   | Message                | Explanation  |
|-----|------------------------|--|
| 242 | Disk Almost Full       | Disk space at value of DISKWARN parameter (usually 90% full).                  |
| 250 | Over Max Key Limit     | Attempt made to download more keys than the device will hold.                  |
| 300 | RDI Full               | RDI transaction buffer full.   |
| 301 | RDI Too Hot            | RDI upper temperature limit exceeded.  |
| 302 | RDI Too Cold           | RDI lower temperature limit exceeded.  |
| 303 | RDI Timeout Problem    | RDI unable to communicate with 808S.   |
| 304 | RDI Hardware Problem   | RDI has detected an error with its operating hardware.                         |
| 305 | RDI Modem Problem      | RDI has detected a modem error.  |
| 306 | RDI Alarm Table Error  | RDI alarm table full or unusable.  |
| 307 | RDI Comm Error         | RDI unable to dial out.  |
| 308 | RDI Host Comm Error    | RDI unable to receive.   |
| 309 | RDI Can't Close 808 DB | RDI unable to complete data transfer to 808S; device left in incomplete state. |
| 500 | Debug 0 Transaction    | WSE development use only.  |
| 501 | Debug 1 Transaction    | •  |
| 502 | Debug 2 Transaction    | •  |
| 503 | Debug 3 Transaction    | •  |
| 504 | Debug 4 Transaction    | •  |
| 505 | Debug 5 Transaction    | •  |

| <b>Message</b>                | <b>#</b> | <b>Message</b>                 | <b>#</b> |
|-------------------------------|----------|--------------------------------|----------|
| ABA Card Data 1 .....         | 173      | Door Report Shunted .....      | 112      |
| ABA Card Data 2 .....         | 174      | Door Report Unshunted .....    | 113      |
| ABA Card Data 3 .....         | 175      | Enter Attended Mode .....      | 82       |
| ABA Card Data 4 .....         | 176      | Enter Unattended Mode .....    | 83       |
| ABA Card Data 5 .....         | 177      | Error .....                    | 221      |
| ABA Card Expired .....        | 172      | Error Dialing Remote .....     | 66       |
| Access Granted .....          | 1        | Error on Device Reset .....    | 158      |
| Access Requested .....        | 21       | Error on Key Reset .....       | 159      |
| Acknowledge DB Xfer .....     | 73       | Error Setting Bldg. Mode ..... | 59       |
| Alarm Acknowledged .....      | 241      | Failed DB Xfer .....           | 74       |
| Alarm Active .....            | 92       | Forgive Passback .....         | 133      |
| Alarm Clear .....             | 93       | General Cancel Report .....    | 211      |
| Alarm Not Acknowledged .....  | 240      | General Closing Report .....   | 209      |
| Alarm Resolved .....          | 81       | General Opening Report .....   | 207      |
| Alarm Silenced .....          | 132      | General Restoral Report .....  | 204      |
| Auto Forgive .....            | 148      | General Trouble .....          | 201      |
| Auto Lock .....               | 16       | Global Silence Request .....   | 86       |
| Auto Unlock .....             | 15       | Host Comm. Started .....       | 26       |
| Batch Request Received .....  | 84       | Host Comm. Stopped .....       | 27       |
| Below Lot Limit .....         | 88       | Host Dial OK .....             | 65       |
| Below Tenant Limit .....      | 87       | Host Dial Start .....          | 142      |
| Bldg Closed .....             | 126      | Host Poller Down .....         | 72       |
| Bldg Opened .....             | 124      | Input Point Active .....       | 43       |
| Bldg Opened Limited .....     | 125      | Input Point Normal .....       | 44       |
| Bldg Should be Closed .....   | 127      | Invalid Card Type .....        | 161      |
| Building Closed .....         | 105      | Invalid Day .....              | 5        |
| Building Open .....           | 103      | Invalid Facility Code .....    | 12       |
| Building Open Limited .....   | 104      | Invalid PIN Entered .....      | 69       |
| Busy Seconds .....            | 220      | Invalid Project .....          | 233      |
| Can't Close Bldg (Key) .....  | 128      | Invalid Reader .....           | 6        |
| Can't Close Bldg - User ..... | 129      | Invalid Site Code .....        | 171      |
| Carrier Off .....             | 143      | Invalid T & A Request .....    | 134      |
| Carrier On .....              | 144      | Invalid Time .....             | 4        |
| Chksum Err In Key DB .....    | 91       | Key Activated .....            | 60       |
| Chksum Err In Sys DB .....    | 90       | Key Deactivated .....          | 61       |
| COAX Failure .....            | 36       | Key Not Active .....           | 62       |
| COAX OK .....                 | 37       | Key Not Active Yet .....       | 7        |
| COAX Report Shunted .....     | 116      | Key Not On File .....          | 11       |
| COAX Report Unshunted .....   | 117      | Key Terminated .....           | 8        |
| Communicator Power Fail ..... | 217      | Key Trace .....                | 2        |
| Database Error .....          | 99       | Keyholder Duress .....         | 76       |
| Debug 0 Transaction .....     | 500      | Line Card Restored .....       | 206      |
| Debug 1 Transaction .....     | 501      | Line Card Trouble .....        | 203      |
| Debug 2 Transaction .....     | 502      | Line Cut .....                 | 162      |
| Debug 3 Transaction .....     | 503      | Line Short .....               | 163      |
| Debug 4 Transaction .....     | 504      | Listen Done .....              | 216      |
| Debug 5 Transaction .....     | 505      | Listen-In Report .....         | 215      |
| Deferred Key .....            | 147      | Logs Purged .....              | 145      |
| Device Cannot Connect .....   | 131      | Lot Full .....                 | 79       |
| Device Online .....           | 54       | Manual Access Granted .....    | 53       |
| Device Reset .....            | 30       | Manual Unlock .....            | 13       |
| Disk Almost Full .....        | 242      | Manual Unlock Timed .....      | 52       |
| Door Closed (Forced) .....    | 19       |                                |          |
| Door Closed (Held) .....      | 20       |                                |          |
| Door Forced Open .....        | 17       |                                |          |
| Door Held Open .....          | 18       |                                |          |

| <b>Message</b>                  | <b>#</b> | <b>Message</b>                | <b>#</b> |
|---------------------------------|----------|-------------------------------|----------|
| Max Tenant In Lot .....         | 80       | Remote Comm Ended .....       | 85       |
| Meal Counter - Excp. ....       | 136      | Remote Trans Received .....   | 64       |
| Meal Counter - Valid .....      | 137      | Repack OK .....               | 58       |
| MSM Fail .....                  | 110      | Req. Passback Forgive .....   | 150      |
| MSM Okay .....                  | 111      | Request Manual Access .....   | 55       |
| MSM Report Shunted .....        | 120      | Request Reset Device .....    | 154      |
| MSM Report Unshunted .....      | 121      | Request Reset Keys .....      | 155      |
| Negative Acknowledge .....      | 0        | Request To Exit .....         | 108      |
| New Day .....                   | 63       | Reset Device Okay .....       | 156      |
| No Key Set for PIN .....        | 75       | Reset Key Okay .....          | 157      |
| Not Used .....                  | 50       | Return From Failsoft .....    | 31       |
| Not Used .....                  | 51       | REX Denied .....              | 109      |
| Not Used .....                  | 96       | Sensor Failure .....          | 38       |
| Open Cash Drawer .....          | 160      | Sensor OK .....               | 39       |
| Output Activated .....          | 67       | Sensor Report Shunted .....   | 118      |
| Output Deactivated .....        | 68       | Sensor Report Unshunted ..... | 119      |
| Over Device Limit .....         | 170      | Shunt Point .....             | 94       |
| Over Max Key Limit .....        | 250      | Status Report .....           | 219      |
| Parameter Load Error .....      | 97       | Still Held Open .....         | 42       |
| Passback Violation .....        | 100      | Tamper Active .....           | 34       |
| Point Disabled .....            | 9        | Tamper Clear .....            | 35       |
| Point Not On File .....         | 10       | Tamper Report Shunted .....   | 106      |
| Point Trace .....               | 3        | Tamper Report Unshunt .....   | 107      |
| Poller Can't Open Port .....    | 23       | Terminal Buffer Full .....    | 130      |
| Poller Died .....               | 22       | Threshold Met .....           | 146      |
| Poller Params Reloaded .....    | 41       | Ticket Serviced .....         | 89       |
| Poller Started .....            | 24       | Time & Attendance Clock ..... | 135      |
| Poller Stopped .....            | 25       | Timeout Device .....          | 45       |
| Power Failed .....              | 32       | Timer Cancelled .....         | 152      |
| Power Report Shunted .....      | 114      | Timer Expired .....           | 153      |
| Power Report Shunted .....      | 122      | Timer Started .....           | 151      |
| Power Report Unshunted .....    | 115      | Tran File Almost Full .....   | 98       |
| Power Report Unshunted .....    | 123      | Unable to Act. Output .....   | 49       |
| Power Restored .....            | 33       | Unable to Clear Output .....  | 48       |
| Power Up Message .....          | 222      | Unable to Lock Door .....     | 46       |
| Printer Error .....             | 40       | Unable to Unlock Door .....   | 47       |
| Printer Off .....               | 28       | Unshunt Point .....           | 95       |
| Printer On .....                | 29       | User Logged Into Term .....   | 140      |
| Project Activated .....         | 230      | User Logged Off Term .....    | 141      |
| Project Deactivated .....       | 231      | VIP Failure .....             | 178      |
| Project Normalized .....        | 232      | VIP Okay .....                | 179      |
| Radionics Unit Power Fail ..... | 213      | VIP Shunted .....             | 182      |
| Radionics Unit Restore .....    | 214      | VIP Tamper Fail .....         | 180      |
| Radionics Unit Test .....       | 200      | VIP Tamper Okay .....         | 181      |
| RDI Alarm Table Error .....     | 306      | VIP Tamper Shunted .....      | 184      |
| RDI Can't Close 808 DB .....    | 309      | VIP Tamper Unshunted .....    | 185      |
| RDI Comm Error .....            | 307      | VIP Unshunted .....           | 183      |
| RDI Dialed In .....             | 78       | Was Forced Armed .....        | 218      |
| RDI Hardware Problem .....      | 304      | Zone Cancel Report .....      | 212      |
| RDI Host Comm Error .....       | 308      | Zone Closed .....             | 210      |
| RDI Is Full .....               | 300      | Zone Count Reset .....        | 149      |
| RDI Is Too Cold .....           | 302      | Zone Opening Report .....     | 208      |
| RDI Is Too Hot .....            | 301      | Zone Restoral .....           | 205      |
| RDI Modem Problem .....         | 305      | Zone Trouble .....            | 202      |
| RDI Timeout Problem .....       | 303      |                               |          |
| Redundancy Off .....            | 71       |                               |          |
| Redundancy On .....             | 70       |                               |          |

**Level 1 = COMPLETE SYSTEM ACCESS**

|          |                           |   |   |          |                           |                           |   |   |   |
|----------|---------------------------|---|---|----------|---------------------------|---------------------------|---|---|---|
|          |                           |   |   | dkrcrprt | DKR Configuration         | N                         | N | N |   |
|          |                           |   |   | downcln  | Download Clean Up & Retry | N                         | N | N |   |
| ID1_entr | ID Security User Entry    | Y | Y | Y        | downrprt                  | Download Status           | N | N | N |
| ID1_rprt | ID Security Report        | N | N | N        | drawmaps                  | Maps                      | N | N | N |
| ID2_entr | ID Security Group Entry   | Y | Y | Y        | egrpcopy                  | Copy Keyholder Access     | N | N | N |
| ID_menu  | ID Security Report        | N | N | N        | egrpentr                  | Access Assignment         | Y | Y | Y |
| aassmenu | Access Assignments        | N | N | N        | egrprprt                  | Keyholder Access Assign   | N | N | N |
| abacentr | ABA Configuration Entry   | Y | Y | Y        | emp_dnld                  | Keyholder Transfer        | N | N | N |
| abacrprt | ABA Configuration         | N | N | N        | emrdrprt                  | Reader Access Assignment  | N | N | N |
| acc_menu | Access Definition         | N | N | N        | epj_rprt                  | Employee Project Report   | N | N | N |
| accrmenu | Access Definition         | N | N | N        | evenentr                  | Events                    | Y | Y | Y |
| accsarch | Access Ctrl Trans Arch    | N | N | N        | evptrprt                  | Event / Point Report      | N | N | N |
| accsmenu | Security Management Rpts  | N | N | N        | excprprt                  | Selective Transaction     | N | N | N |
| acdsentr | Access Code Entry         | Y | Y | Y        | exit                      | Exit SE / SMS Application | N | N | N |
| acodrprt | Access Code Master Rpt    | N | N | N        | fmntmenu                  | Master File Entry         | N | N | N |
| acoventr | Access Override Entry     | Y | Y | Y        | fs_entr                   | Fail Soft Entry           | Y | Y | Y |
| acovrprt | Access Override Report    | N | N | N        | fs_rprt                   | Fail Soft Report          | N | N | N |
| acrtrprt | Access Control Archive    | N | N | N        | hol_entr                  | Holidays                  | Y | Y | Y |
| addusers | Addusers                  | N | N | N        | hol_rprt                  | Holidays                  | N | N | N |
| agdsentr | Access Group Entry        | Y | Y | Y        | instentr                  | Instructions              | Y | Y | Y |
| agrprprt | Access Group Master Rpt   | N | N | N        | instrprt                  | Instructions              | N | N | N |
| almarprt | Alarm Servicing           | N | N | N        | invtmenu                  | Key Inventory             | N | N | N |
| alotentr | Tenant Allotment          | Y | Y | Y        | job_entr                  | Jobcat                    | Y | Y | Y |
| alrmcln  | Alarm Trans Clean Up      | N | N | N        | job_rprt                  | Jobcat                    | N | N | N |
| areaentr | Areas                     | Y | Y | Y        | josprprt                  | Special Journal Reporting | N | N | N |
| autoentr | Auto Opens / Activates    | Y | Y | Y        | jourarch                  | Journal Archive           | N | N | N |
| autorprt | Auto Opens / Activates    | N | N | N        | jourrprt                  | Journal Reporting         | N | N | N |
| badgarch | Badge Archiving           | N | N | N        | key_copy                  | Copy Keyholders           | N | N | N |
| badgentr | Badge Entry               | Y | Y | Y        | key_entr                  | Keyholders                | Y | Y | Y |
| badgrprt | Print Badges              | N | N | N        | key_rprt                  | Keys Master               | N | N | N |
| badtrprt | Offline Badge Reporting   | N | N | N        | keyload1                  | Keyholder Loading Prog 1  | N | N | N |
| bdg1rprt | Badge Report              | N | N | N        | ktimentr                  | Keyholder Timer Entry     | Y | Y | Y |
| beepentr | Enable Global Beeping     | Y | Y | Y        | kyznrprt                  | Keyholder Zone            | N | N | N |
| bkup     | Perform Backup            | N | N | N        | loadmenu                  | Key Holder Loading        | N | N | N |
| calliq   | Accellq (Custom Reports)  | N | N | N        | loc_entr                  | Location                  | Y | Y | Y |
| casmrprt | Cash Summary              | N | N | N        | loc_rprt                  | Location                  | N | N | N |
| cdinentr | Key Inventory Entry       | Y | Y | Y        | lsumdel                   | Delete Lot Sum Records    | N | N | N |
| cdinrprt | Key Inventory Report      | N | N | N        | lsumentr                  | Daily Lot Summary         | Y | Y | Y |
| chstrprt | Keyholder History Report  | N | N | N        | lsumrprt                  | Daily Lot Summary         | N | N | N |
| compentr | Company                   | Y | Y | Y        | mainmenu                  | SE / SMS Main Menu        | N | N | N |
| comprprt | Company                   | N | N | N        | mangrprt                  | Daily Manager's           | N | N | N |
| con_menu | Device Configuration Rpts | N | N | N        | maprprt                   | Maps                      | N | N | N |
| confmenu | Hardware Configuration    | N | N | N        | mealrprt                  | Meal Report               | N | N | N |
| ctrlentr | Control File Maintenance  | Y | Y | Y        | mlwkrprt                  | Hours vs. Meals Taken     | N | N | N |
| db_menu  | Database Maintenance      | N | N | N        | mnaccopy                  | Copy Security             | N | N | N |
| dbstats  | Display Data Base Stats   | N | N | N        | mod_pass                  | Modify Passwords          | N | N | N |
| dconrprt | 808 Device Configuration  | N | N | N        | monitor                   | Monitor Security Activity | N | N | N |
| deptrprt | Dept                      | Y | Y | Y        | nodeentr                  | SE 422 Hardware Def       | Y | Y | Y |
| deptentr | Dept                      | N | N | N        |                           |                           |   |   |   |
| dev_entr | Devices                   | Y | Y | Y        |                           |                           |   |   |   |
| dev_rprt | Devices                   | N | N | N        |                           |                           |   |   |   |
| dialentr | Dialer Entry              | Y | Y | Y        |                           |                           |   |   |   |
| dialrprt | Dialers                   | N | N | N        |                           |                           |   |   |   |
| dkrcentr | DKR Configuration Entry   | Y | Y | Y        |                           |                           |   |   |   |

|          |                             |   |   |   |                               |                            |   |   |   |
|----------|-----------------------------|---|---|---|-------------------------------|----------------------------|---|---|---|
| outsrpt  | Outstanding Tickets         | N | N | N | taskrpt                       | Task / Event Master Report | N | N | N |
| overrpt  | Tenant Overage              | N | N | N | tatransf                      | Record Transfer            | N | N | N |
|          |                             |   |   |   | tbleentr                      | Rate Tables                | Y | Y | Y |
| p422rpt  | SE/422 PIN Report           | N | N | N | tblrrpt                       | Tenant Billing             | N | N | N |
| padmmenu | Parking Administration      | N | N | N | tententr                      | Tenants                    | Y | Y | Y |
| parkmenu | Parking Control             | N | N | N | tentrprt                      | Tenants                    | N | N | N |
| pgacentr | Security Entry              | Y | Y | Y | termentr                      | Terminal / Point Xref      | Y | Y | Y |
| pgacrprt | Security Master List        | N | N | N | thstrprt                      | Tour Schedule vs Access    | N | N | N |
| phstrprt | Point History               | N | N | N | tickentr                      | Ticket Editing             | Y | Y | Y |
| plotentr | Point/Lot Association       | Y | Y | Y | tickpost                      | Post Serviced Tickets      | N | N | N |
| pndfentr | SE422 PIN Definition        | Y | Y | Y | tickrprt                      | Ticket Transaction Report  | N | N | N |
| pnt_entr | Points                      | Y | Y | Y | timemenu                      | Time & Attendance          | N | N | N |
| pnt_rprt | Points                      | N | N | N | tkeyrprt                      | Keyholder Tour History     | N | N | N |
| pol_entr | Pollers                     | Y | Y | Y | tlogrprt                      | Ticket Log                 | N | N | N |
| pol_rprt | Pollers                     | N | N | N | tmcdentr                      | Time Codes                 | Y | Y | Y |
| prd_rprt | Project Reader Report       | N | N | N | tmcdrprt                      | Time Codes                 | N | N | N |
| prj_entr | Project Definition          | Y | Y | Y | tourmenu                      | Guard Tour                 | N | N | N |
| prj_rprt | Project Report              | N | N | N | tranentr                      | Transactions               | Y | Y | Y |
| psetmenu | Parking Setup               | N | N | N | trdsentr                      | Tour Definition            | Y | Y | Y |
| purgrprt | Purge A Pending Report      | N | N | N | trdsrprt                      | Tour Definition            | N | N | N |
|          |                             |   |   |   | trptmenu                      | Ticket Reports             | N | N | N |
| quckrprt | Quick Ticket Search         | N | N | N | trshentr                      | Tour Scheduling            | Y | Y | Y |
|          |                             |   |   |   | trshrprt                      | Tour Schedule              | N | N | N |
| rdefentr | Device Report Definition    | Y | Y | Y | tsumrprt                      | Daily Ticket Summary       | N | N | N |
| rdefrprt | 808 Report Definition       | N | N | N |                               |                            |   |   |   |
| rdr_entr | Readers                     | Y | Y | Y | usraentr                      | Shift                      | Y | Y | Y |
| rdr_rprt | Readers                     | N | N | N | usrbentr                      | Emp Stat                   | Y | Y | Y |
| rpasrprt | Passback Zone Report        | N | N | N | usrdmenu                      | User Defined Information   | N | N | N |
| rprtmenu | Master File Reports         | N | N | N |                               |                            |   |   |   |
|          |                             |   |   |   | vctlentr                      | Badge Color Entry          | Y | Y | Y |
| sec_menu | Program Security            | N | N | N | vistentr                      | Visitor Entry              | Y | Y | Y |
| sel_entr | Selection Table             | Y | Y | Y | vistmenu                      | Visitors                   | N | N | N |
| service  | Ticket Servicing            | N | N | N | vistrprt                      | Visitor Report             | N | N | N |
| showdate | Display Date & Time         | N | N | N |                               |                            |   |   |   |
| showuser | Display All Valid Logins    | N | N | N | weekentr                      | Week Ending Dates          | Y | Y | Y |
| showwho  | Display All Users Logged In | N | N | N | whowhere                      | Passback Zone              | N | N | N |
| siteentr | Site Entry Definition       | Y | Y | Y |                               |                            |   |   |   |
| siterprt | Site Definition             | N | N | N | zoneentr                      | Zones                      | Y | Y | Y |
| spitentr | Ticket Spitter Synch        | Y | Y | Y | zonerprt                      | Zones                      | N | N | N |
| statentr | Status Code Entry           | Y | Y | Y |                               |                            |   |   |   |
| statmenu | Inventory Stat Code Menu    | N | N | N | <b>Level 2 = MONITOR ONLY</b> |                            |   |   |   |
| statrprt | Status Code Report          | N | N | N |                               |                            |   |   |   |
| stkrentr | Parking Sticker Entry       | Y | Y | Y | exit                          | Exit SE / SMS Application  | N | N | N |
| stkrmenu | Parking Stickers            | N | N | N | mainmenu                      | SE / SMS Main Menu         | N | N | N |
| stkrprt  | Parking Sticker Master Rpt  | N | N | N | monitor                       | Monitor Security Activity  | N | N | N |
| stkrprt  | Parking Sticker Display     | N | N | N |                               |                            |   |   |   |
| summdel  | Delete Ticket Records       | N | N | N |                               |                            |   |   |   |
| syclmenu | System Configuration        | N | N | N |                               |                            |   |   |   |
| sys_menu | System Administration       | N | N | N |                               |                            |   |   |   |
|          |                             |   |   |   |                               |                            |   |   |   |
| taarch   | Transaction Archiving       | N | N | N |                               |                            |   |   |   |
| tacfentr | Conf Early / Late Hours     | Y | Y | Y |                               |                            |   |   |   |
| taentr   | Editing                     | Y | Y | Y |                               |                            |   |   |   |
| taexentr | T & A Exceptions            | Y | Y | Y |                               |                            |   |   |   |
| tairprt  | Keyholder Inquiry           | N | N | N |                               |                            |   |   |   |
| tarprprt | Detail / Summary Report     | N | N | N |                               |                            |   |   |   |
| tartprpt | Offline Reporting           | N | N | N |                               |                            |   |   |   |
| taskentr | Tasks                       | Y | Y | Y |                               |                            |   |   |   |

# INDEX

## A

- Access Assignment, 4-8, 5-4
  - Keyholder Access, 5-4
  - Keyholder Access Assignment, 4-8
  - Readers, 5-5
- Access Code, 1-2
- Access Code Entry, 4-9
  - Distributed Access codes, 4-9
  - Host, 4-9
  - Smart Failsoft, 4-9
- Access Control Archive Report, 3-4
- Access Control Transaction Archiving [accsarch], 6-15
- Access Control Units (ACUs), 1-3
- Access Definition, 4-9, 5-6
  - Access Code Master, 5-6
  - Access Group Master, 5-6
  - Access Override, 5-7
  - Intelligent Failsoft, 5-7
  - Keyholder Projects, 5-9
  - Project Report, 5-8
  - Reader Projects, 5-10
- Access Group, 1-2
- Access Group Entry, 4-11
- Access Override Entry, 4-13
- Activate / Deactivate Codes, 6-11
- ACUs, 1-3
- Add Users [addusers], 6-2
- Adding / Changing Data, 1-14
- Adjustable Baud Rate—708P/800 Pollers, 6-19
- Alarm Contact, 1-2
- Alarm Contacts, 1-4
- Alarm Servicing, 2-8
  - Alarm Servicing Function Keys, 2-8
  - No Activity Timeout, 2-13
- Alarm Servicing Archive Report
  - Sample Report, 3-5
- Alarm Servicing Function Keys, 2-8
- Alarm Servicing Report, 3-4
- Alarm Transaction Clean Up [almcIn], 6-16
- Alarms and Responses, 1-7
- All Transactions, 1-7
- Anti-Passback Control, 1-6
- Application Screens, 1-10
- Audible Alarms, 1-5
- Auto Key Entry, 4-34
  - Automatically Entering Card Numbers, 4-34
  - Configuring the Reader, 4-34

Auto Opens/Activates, 4-42  
Automatic Access Control, 1-6  
Automatic Activate / Deactivate, 1-6  
Automatic Restart, 1-16  
Automatic Unlock/Lock, 1-6

## **B**

Basic System Usage, 1-16  
    Logging Off, 1-15  
Biometric Identifiers, 1-3  
Building Modes, 2-11

## **C**

CCTV, 1-17  
Clearing a Field, 1-14  
Communications Monitor, 1-6  
Company, 1-2  
Complete Portability, 1-5  
Contact Alarms, 1-4  
Control Building Modes Function Keys, 2-11  
Control Devices Function Keys, 2-3  
Control Devices screen, 2-3  
Control Doors Function Keys, 2-6  
Control File Maintenance [ctrlentr], 6-8  
Control Function Keys  
    Control Doors Function Keys, 2-6  
    Control Input Function Keys, 2-5  
    Control Locks Function Keys, 2-4  
    Control Output Function Keys, 2-5  
    Control Zone Function Keys, 2-6  
    Locks, 2-4  
Control Function Menu  
    Devices, 2-3  
Control Functions Menu, 2-2  
    Poller Function Keys, 2-2  
    Pollers, 2-2  
Control Inputs Function Keys, 2-5  
Control Locks Function Keys, 2-4  
Control Outputs Function Keys, 2-5  
Control Pollers Function Keys, 2-2  
Control Printers Function Keys, 2-9  
Control Projects, 2-9  
    Control Projects Function Keys, 2-9  
Control Remote Devices Function Keys, 2-11  
Controller Systems, 1-18  
Copy Keyholder Access, 4-8  
Copy Keyholders, 4-7  
Copy Security [mnaccopy], 6-6

**D**

- Data Entry Sequence, 1-9
- Data Item Selection, 2-2
- Database Changes, 1-7
- Database Maintenance [db\_menu], 6-14
- Definition, General
  - Trace, 1-3
  - Transactions, 1-3
- Definition, Inputs
  - Fire Alarms/Heat Sensors, 1-4
- Definition, Principal System Functions
  - Auto Unlock/Lock, 1-6
- Definitions
  - Access Control, 1-6
- Definitions, Basic System Usage, 1-9
  - Applications Screens, 1-10
  - Logging On, 1-9
  - System Screens, 1-10
- Definitions, Creating the Database, 1-8
  - Poller Initializatin, 1-8
- Definitions, File Maintenance, 1-7
- Definitions, General, 1-2
  - Access Code, 1-2
  - Access Group, 1-2
  - Alarm Contract, 1-2
  - Company, 1-2
  - Department, 1-2
  - Device, 1-2
  - Event, 1-2
  - Job Category, 1-2
  - Key Number, 1-2
  - Keyholder ID, 1-3
  - Location, 1-3
  - Time Code, 1-3
  - Zones, 1-3
- Definitions, Hardware
  - Devices, 1-3
  - Microprocessor, 1-3
- Definitions, Inputs, 1-4
  - Alarm Contacts, 1-4
  - Contact Alarms, 1-4
  - Door Switches, 1-4
  - Intrusion Devices, 1-4
  - Motion Sensors, 1-4
  - Multiple Switch Monitor, 1-5
  - Points, 1-5
  - Request-to-Exit, 1-5
  - Video Monitor Switchers, 1-4
- Definitions, Outputs, 1-5
  - Audible Alarms, 1-5
  - Remote Alarms, 1-5

- Definitions, Principal System Functions, 1-6
  - Auto Activate/Deactivate, 1-6
  - Automatic Access Control, 1-6
  - Communications Monitor, 1-6
  - Flexible Event Handling, 1-6
  - Independent PIN Entry, 1-6
  - Manual Access Control, 1-6
  - Two-Man Rule, 1-6
- Definitions, Readers, 1-4
  - Digital Key Reader, 1-4
  - Magnetic Card Reader, 1-4
  - Readers, Sensors, 1-4
- Definitions, Reporting, 1-7
  - Alarms and Responses, 1-7
  - All Transactions, 1-7
  - Database Changes, 1-7
  - Invalid Access Attempts, 1-7
  - Keyholder History, 1-7
  - Point History, 1-7
- Definitions, System Function
  - Anti-Passback Control, 1-6
- Definitions, System Software, 1-5
  - Installation Flexibility, 1-5
  - Integrated Software, 1-5
  - Open System Design, 1-5
  - Portability, 1-5
  - Response Time, 1-6
- Definitions, Tenant, 1-3
- Deleting a Character in a Field, 1-14
- Deleting Records, 1-14
- Department, 1-2
- Device, 1-2
- Device Configuration Reports, 5-13
  - 422 PIN Master, 5-20
  - 808, 5-17
  - 808 Configuration, 5-18
  - ABA Configuration, 5-19
  - Auto Opens/Activates, 5-17
  - Dialers, 5-18
  - DKR Configuration, 5-20
  - Points, 5-16
  - Pollers, 5-14
  - Site Definition, 5-18
  - Zones, 5-13
- Devices
  - 422 Device Configuration Entry, 4-28
  - 422 Reader Report Defined, 4-36
  - 818 Device Configuration Entry, 4-28
  - 818 Reader Report Defined, 4-37
  - 8xx-Series Reader Report, 4-35
  - Auto Key Entry, 4-34
  - Device Entry Screen, 4-22

- NexSentry Reader Report Defined, 4-38
- Reader Entry, 4-32
- Reader Report, 4-35
- Readers, 4-31
- Devices Configuration Reports
  - Devices, 5-14
  - Readers, 5-15
- Digital Key Reader, 1-4
- Disk Almost Full Warning, 2-12
- Display All Users Logged In [showwho], 6-7
- Display All Valid Logins [showuser], 6-7
- Display Current Date and Time [showdate], 6-7
- Display Database Statistics [dbstats], 6-14
- Distributed Access Codes, 4-9
- Documentation Methods, 1-2
- Door switches, 1-4
- Doors, 2-6
- Download Clean Up and Retry [downcln], 6-15
- Download Status
  - Before Transmission, 3-7
  - Error in Receiving Data, 3-7
  - Error in Transmitting Data, 3-7
  - Received and Processed, 3-7
  - Transmitted, 3-7
  - Unprocessed, 3-7
- Download Status Report, 3-6
  - Sample Report, 3-7

## E

- Elevator Control, 1-18
- Elevator Definition, 4-11
- Enable Terminals for Global Beeping [beepentr], 6-8
- Event, 1-2
- Event Monitoring, 1-6
- Event/Point Report, 3-8
  - Sample Report, 3-9
- Events [evenentr], 6-9

## F

- Failsoft, 4-14
- File Maintenance, 1-7
- Finding, Adding, and Storing Data, 1-13
  - Adding/Changing Data, 1-14
  - Searching, Partial Information, 1-13
  - Storing Data, 1-14
- Finding Data, 1-13
- Fire Alarms, 1-4
- Fire Alarms / Heat Sensors, 1-4
- Flexible Event Handling, 1-6
- Following the System Interconnect Diagram, number, 1-9
- Force Table Download, 2-10

Forgive Passback, 2-10  
Full Screen Monitoring, 2-12  
Function Keys, 2-2

## G

General Definitions  
Keyholder, 1-2  
Guard Tour, 1-18

## H

Hardware Configuration  
422 Hardware Definition, 4-44  
Hardware Configuration  
422, 4-28  
422 Pin Definition, 4-43  
818, 4-28  
8xx Series, 4-24  
ABA Configuration, 4-47  
Areas, 4-19  
Device Report, 4-43  
Devices, 4-21  
Dialer Entry, 4-45  
DKR Configuration, 4-48  
NexSentry, 4-26  
Points, 4-39  
Pollers, 4-19  
Readers, 4-31  
Site Entry Definition, 4-46  
Zones, 4-18  
Heat Sensors, 1-4  
Holidays, 4-16, 5-11

## I

ID Security Group Entry [ID2\_entr], 6-18  
ID Security Maintenance [ID\_menu], 6-17  
ID Security Report [ID1\_rprt], 6-18  
ID Security User Entry [ID1\_entr], 6-17  
ID-4000 Interface, 1-18  
Independent PIN Entry, 1-6  
Input Points, 2-5  
Installation Flexibility, 1-5  
Integrated Software Support, 1-5  
Intelligent Devices, 4-21  
Intrusion Devices, 1-4  
Invalid Access Attempts, 1-7  
Inventory Status Code Menu [statentr], 6-20  
IQ, 1-17

**J**

Job Category, 1-2  
Journal Archive [jourarch], 6-16  
Journal Reporting [jourrprt], 6-16

**K**

Key Inventory [invtmnu], 6-20  
Key Inventory Entry [cdinentr], 6-21  
Key Inventory Report [cdinrprt], 6-21  
Key Inventory Status Code Report [statrprt], 6-20  
Key Number, 1-2  
Keyholder, 1-2

- Access Assignment, 4-8
- Keyholder Access Entry, 4-5
- Keyholder Entry, Page 1, 4-2
- Keyholder Entry, Page 2, 4-4
- Master Reports, 5-2
- Project Assignment, 4-6

Keyholder History, 1-7  
Keyholder History Report, 3-2

- Sample Report, 3-3

Keyholder ID, 1-3  
Keyholder Loading [loadmenu], 6-17  
Keyholder Zone Report, 3-8

- Sample Report, 3-8

Keyholders, 4-2  
Keypad Controllers, 1-4  
Keys Master, 5-2

**L**

Location, 1-3  
Locks, 2-4  
Logging Off, 1-15  
Logging On, 1-9

**M**

Magnetic Card Readers, 1-4  
Manual Access Control, 1-6  
Manual Access Granted, 2-10  
Manual Organization, 1-1

- Documentation Methods, 1-2
- System Main Menu, 1-1

Manual Restart, 1-16  
Maps, 4-50, 5-13

- Map Drawing, 4-50

Master File Entry, 4-1  
Master File Reports, 5-1  
Menu Screens, 1-10

Microprocessor  
    Access Control Units, 1-3  
    Biometric Hand Reader, 1-3  
Miscellaneous Information, 1-15, 2-12  
Modified Usage of Invalid Facility Code Log, 2-15  
Modify Passwords [mod\_pass], 6-4  
Monitor Security Activity, 2-1  
Monitoring Security - Passwords, 2-14  
Motion Sensors, 1-4  
Moving Backwards in a Field, 1-14  
Moving Between Data Fields, 1-12  
Moving to Prior Screens, 1-13  
MSMs, 1-5  
Multiple Switch Monitors (MSMs), 1-5

## O

Open System Design, 1-5  
Optional Features, 1-17  
    CCTV, 1-17  
    Controller Systems, 1-18  
    Elevator Control, 1-18  
    Guard Tour, 1-18  
    ID-4000, 1-18  
    IQ, 1-17  
    Parking Control, 1-18  
    Remote RDI, 1-18  
    Time and Attendance, 1-18  
    Visitor Control, 1-18  
Other Functions, 2-9  
    Printer Control, 2-9  
Output Points, 2-5

## P

Parking Control, 1-18  
Parking Sticker Entry [stkrentr], 6-22  
Parking Sticker Interactive Display [stkrprt1], 6-22  
Parking Sticker Master Report [stkrprt], 6-23  
PARKING STICKERS [stkrmenu], 6-22  
Passback Zone Report, 3-5  
    Sample Report, 3-6  
Perform Backup [bkup], 6-14  
Point History, 1-7  
Point History Report, 3-2  
    Sample Report, 3-2  
Points, 1-5, 4-39  
Poller Initialization Parameters Information, 1-8  
Pollers, 2-2  
Pollers Function Keys, 2-2  
Powering On the System, 1-16  
Program Security [sec\_menu], 6-5

Program Security Entry Definition [pg1\_entr], 6-5  
Purge a Pending Report [purgrprt], 6-8

## R

Reader Entry, 4-32  
Reader Report, 4-35  
    818, 4-37  
    NexSentry, 4-38  
Reader Report, 422, 4-36  
Readers, 1-4  
Real Time Control Maps, 2-8  
Realtime Passback Zone Report, 3-9  
Remote Alarms, 1-5  
Remote Devices, 2-11  
Remote Dial-Up Interface, 1-18  
Reporting, 1-7  
Reports  
    132-Column, 5-21  
    ABA Configuration, 5-19  
    Access Code Master List, 5-6  
    Access Group Master List, 5-7  
    Access Override, 5-7  
    Auto Open/Activate, 5-17  
    Company, Dept, 5-12  
    Devices, 5-15  
    Dialers, 5-18  
    DKR Configuration, 5-20  
    Holiday Codes, 5-11  
    Intelligent Fail Soft, 5-8  
    Keyholder Access Assignment, 5-4  
    Keyholder Projects, 5-9  
    Keys Master, 5-2  
    Maps, 5-13  
    Points, 5-16  
    Pollers, 5-14  
    Projects, 5-9  
    Reader Assignment, 5-5  
    Reader Project, 5-10  
    Readers, 5-16  
    SE 422 PIN, 5-21  
    SE 808, 5-17  
    Sites, 5-19  
    Tenants, 5-12  
    Time Codes, 5-11  
    Zones, 5-14  
Request-to-Exit (REX) Sensor, 1-5  
Restarting The System  
    Automatic Restart, 1-16  
    Manual Restart, 1-16  
Restarting the System, 1-16

Review Transactions  
    Full Screen, 2-7  
Review Transactions Function Keys, 2-8  
REX, 1-5

## **S**

Sample System, 1-7  
Screen Access, 4-1  
Screen Examples, 1-11  
Searching With Partial Information, 1-13  
Section Organization, 2-1  
Security Master List [pgacrprt], 6-6  
Security Reports, 3-1  
Select Zone, 2-6  
Select Zone Function Keys, 2-6  
Selecting Screens, 1-12  
Shutting Down, 1-16  
Signature Verify, 1-9  
Silence Beeps, 2-9  
Simple Devices, 4-21  
Smart Failsoft Access Codes, 4-9  
Special Journal Reporting [josrprt], 6-16  
Status Screen Function Timeout, 2-13  
Storing Data, 1-14  
System Administration  
    Add Users, 6-2  
    Database Maintenance, 6-14  
    Display All Users Logged In, 6-7  
    Display All Valid Logins, 6-7  
    Display Current Date and Time, 6-7  
    Enable Terminals for Global Beeping, 6-8  
    ID Security Maintenance, 6-17  
    Keyholder Loading, 6-17  
    Miscellaneous Information, 6-19  
    Modify Passwords, 6-4  
    Program Security, 6-5  
    Purge Pending Report, 6-8  
    System Configuration, 6-8  
System Configuration (syclmenu), 6-8  
System Interconnect Diagram, 1-8  
System Main Menu, 1-1  
System Monitoring, 2-1  
System Screen Trees, 1-17  
    See also Appendix A, 1-17  
    See Also Appendix B, 1-17  
System Screens, 1-10  
System Software, 1-5

## **T**

Task Event / Master Report [taskrprt], 6-12  
Tasks, 6-10

Tenant, 1-3  
Tenants, 4-17, 5-11  
Time and Attendance, 1-18  
Time Code, 1-3  
Time Codes, 4-16, 5-10  
Trace, 1-3  
Transaction History Report, 3-3  
    Sample Report, 3-4  
Transactions, 1-3  
Transactions [tranentr], 6-12  
Two-Man Rule, 1-6

## **U**

User Defined Information, 4-49  
Using Screens and Fields, 1-12  
    Moving Between Data Fields, 1-12  
    Moving to Prior Screens, 1-13  
    Selecting Screens, 1-12

## **V**

Video Monitor Switchers, 1-4  
Visitor Control, 1-18

## **W**

Watch Dog Timer Count, 4-23

## **Y**

Y, 1-12

## **Z**

Zones, 1-3, 4-18  
Zoom  
    Canceling Zoom, 1-15  
Zoom Feature, 1-15