

Security Escort



Security Systems

EN

Technical Reference
Manual
Security Escort

BOSCH

Software License Agreement

Security Escort's Central Control Software for Microsoft® Windows®.

Microsoft®, Windows®, Windows NT® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.



This software relates to security. Access should be limited to authorized individuals. This software contains provisions for setting security passwords. Appropriate security levels should be established and passwords should be set before allowing operating personnel access to this software. The original disk should be safeguarded against unauthorized use. In addition, DS security/fire controls contain passwords to prevent unauthorized access; these passwords must also be set and their identity carefully safeguarded.

Please read the following license agreement prior to installing and operating the software. Do not install this software unless you agree to the following terms:

You MAY

- Use the Security Escort program only on a single Security Escort system, with a single master computer, a single optional slave computer, and only the number of workstations originally factory programmed into the software key.
- This program can be used without a software key only for demo purposes. In no case can this program be used on a live system without an authorized software key.
- Copy the program into another computer only for backup purposes in support of your use of the program on one Security Escort system.

You may NOT

- Transfer this program or license to any other party without the express written approval of Bosch Security Systems.

Limited Warranty

Bosch Security Systems warrants that the program will substantially conform to the published specifications and documentation, provided that it is used on the computer hardware and with the operating system for which it was designed. Bosch Security Systems also warrants that the magnetic media on which the program is distributed and the documentation are free of defects in materials and workmanship. No Bosch Security Systems dealer, distributor, agent, or employee is authorized to make any modification or addition to this warranty, oral, or written. Except as specifically provided above, Bosch Security Systems makes no warranty or representation, either express or implied, with respect to this program or documentation, including their quality, performance, merchantability, or fitness for a particular purpose.

Remedy

Bosch Security Systems will replace defective media or documentation, or correct substantial program errors at no charge, provided you return the item with proof of purchase to Bosch Security Systems within 90 days of the date of delivery. If Bosch Security Systems is unable to replace defective media or documentation, or correct substantial program errors, Bosch Security Systems will refund the license fee. These are your sole remedies for any breach of warranty.

Because programs are inherently complex and may not be completely free of errors, you are advised to verify your work. In no event will Bosch Security Systems be liable for direct, indirect, incidental, or consequential damages arising out of the use of or inability to use the program or documentation, even if advised of the possibility of such damages. Specifically, Bosch Security Systems is not responsible for any costs including, but not limited to, those incurred as a result of lost profits or revenue, loss of use of the computer programs or data, the cost of any substitute program, claims by third parties, or for other similar costs. Bosch Security Systems does not represent that the licensed programs may not be compromised or circumvented. In no case shall Bosch Security Systems liability exceed the amount of the license.

Some states do not allow the exclusion or limitation of implied warranties, or limitation of liability for incidental or consequential damages, so the above limitation or exclusion may not apply to you.

Bosch Security Systems retains all rights not expressly granted. Nothing in this license constitutes a waiver of Bosch Security Systems rights under the U.S. Copyright laws or any other Federal or state law.

Should you have any questions concerning this license, write to: Bosch Security Systems, 130 Perinton Parkway, Fairport, New York 14450.

Table of Contents

1.0 Security Escort System Architecture	7	3.3.7 Communications Port Monitor ...	42
1.1 System Components.....	7	3.3.8 Delay To Ignore Troubles That Auto Reset	42
1.1.1 System Overview.....	7	3.3.9 Transponder Communications Screen	42
1.1.2 Transmitter.....	7	3.3.10 Transponder Current Status Screen	45
1.1.3 Receiver.....	8	3.3.11 Transponder Parameter Change Screen	47
1.1.4 Alert Unit.....	8	3.3.12 Transponder Data View Screen .	48
1.1.5 Transponder.....	9	3.3.13 Receiver Configuration Screen	49
1.1.6 Central Console.....	9	3.3.14 Receiver Test Screen	51
1.1.7 Software Overview.....	9	3.3.15 Network Status Screen	52
1.2 System Operation.....	10	3.3.16 System Status Screen	53
1.2.1 Alarm Sequence.....	10	3.3.17 System Preferences Screen	54
1.2.2 Test Sequence.....	12	3.3.18 Transponder Comm Port Setup Screen	57
2.0 Setting Up The System	13	3.3.19 Remote Comm Port Setup Screen	58
2.1 Initial System Configuration...	13	3.3.20 Remote Setup Screen	59
3.0 System Menus and Screens	13	3.3.21 Remote Connection Screen	60
3.1 File Menu.....	13	3.3.22 Phone Book Edit Screen	61
3.1.1 Locate Transmitters.....	13	3.3.23 Pager Setup Screen	62
3.1.2 Maintenance Alarm Database.....	14	3.3.24 Send Pager Message Screen	63
3.1.3 Operator Database.....	14	3.4 Printer Menu	63
3.1.4 Reports Database.....	14	3.4.1 Select Alarm Printer Screen ...	64
3.1.5 Subscriber Database.....	14	3.4.2 Select Report Printer Screen Screen	64
3.1.6 Transponder Database.....	17	3.4.3 Print History Screen	64
3.1.7 Creating a New Transponder Entry.	19	3.4.4 Print File Screen	64
3.1.8 Setting Receiver Parameters....	20	3.5 Network Menu	65
3.1.9 Transmitter Change.....	26	3.5.1 System Directories and Network Address Screen	65
3.1.10 Exit.....	26	3.5.2 Network Socket Status Screen ..	67
3.2 Utilities Menu.....	26	3.5.3 Winsock Data Screen	68
3.2.1 Backup Screen.....	26	3.5.4 This Computer's Name and Address Screen	68
3.2.2 Restore Screen.....	27	3.6 About Menu	68
3.2.3 Security Preferences Screen....	28	3.6.1 About Screen	69
3.2.4 System Defaults Screen.....	31	4.0 Files Required For Security Escort	70
3.2.5 System Labels Screen.....	31	5.0 Image Files	71
3.2.6 Print System Reports Screen....	31	5.1 Map File Generation and Scaling	71
3.2.7 Alarm Report Generation Screen.	32	5.2 Multiple Map Files	72
3.2.8 Schedules Screen.....	33	5.3 Subscriber Images	72
3.2.9 Edit Schedule Times Screen.....	34	6.0 Security Escort Pager Setup ...	72
3.2.10 View Alarm Groups Screen.....	34	6.1 Dial-up Paging Modem Setup	73
3.2.1 Alarm Groups Screen.....	35	6.2 Local Paging Setup	73
3.2.12 Alarm Group State Screen.....	35	6.3 Service and Security (Alarm) Pager Setup	74
3.2.13 Current Check-in Status Screen	36	6.4 Subscriber (Individual) Pager Setup	74
3.2.14 Clear Screen.....	36	6.5 Alarm Area Setup	75
3.2.15 Output Verification.....	36	6.6 Manual Pages	75
3.2.16 Synchronize System Time.....	36	7.0 Importing a Subscriber Database	76
3.3 Setup Menu.....	36		
3.3.1 Show History.....	36		
3.3.2 History Filter Screen.....	37		
3.3.3 Popup Trouble Filter.....	39		
3.3.4 Transponder Troubles.....	40		
3.3.5 Mux Bus Point Troubles.....	41		
3.3.6 Transmitter Supervision Monitor	41		

Figures

Figure 1: Screen Box for Password Entry	10	Figure 33: Edit Schedule Time Screen	34
Figure 2: Central Console Screen During Alarm.....	11	Figure 34: View Alarm Groups Screen .	34
Figure 3: Console Screen Showing test Icons.....	12	Figure 35: Alarm Groups Screen	35
Figure 4: File Menu	13	Figure 36: Alarm Group State Screen .	35
Figure 5: Locate Transmitters	14	Figure 37: Current Check-in Status Screen	36
Figure 6: Maintenance alarm with Signal Levels Shown in Icons".....	14	Figure 38: Setup Menu.....	36
Figure 7: Edit Subscriber's Advanced Features Screen.....	14	Figure 39: History Filter Screen	37
Figure 8: Find Transponder's Database Record.....	17	Figure 40: Pop-Up Alert Showing Receiver not Responding	39
Figure 9: Blank Screen Resulting from Selecting the Insert New Button.....	20	Figure 41: Pop-up Trouble Filter Screen	39
Figure 10: Select Point Screen with "All Points" Selected.....	20	Figure 42: Transponder Communications Screen	42
Figure 11: Select Point Screen with "Receivers Only" Selected...	21	Figure 43: Transponder Current Status Screen	45
Figure 12: Drop-Down Menu for Selection of Point Type.....	21	Figure 44: Transponder Parameter Change Screen	47
Figure 13: Data Entry After Selection of Receiver Point Type.....	22	Figure 45: Transponder Data View Screen	48
Figure 14: Data Entry after Selection of Alert Unit Point Type.....	22	Figure 46: Receiver Configuration Screen	49
Figure 15: Data Entry after Selection of Virtual Receiver Point Type.	22	Figure 47: Abort Button to Remove a Device from the Setup Mode .	50
Figure 16: Data Entry when Show Areas is Selected	22	Figure 48: Confirmation of Successful Setup Test	50
Figure 17: Drop-Down Menu for Assigning Alert Units to Receivers....	23	Figure 49: Receiver Test Screen	51
Figure 18: Location Algorithm Selection	23	Figure 50: Network Status Screen	52
Figure 19: Receiver floor level selection.....	23	Figure 51: System Status Screen	53
Figure 20: Save Changes Screen Box ...	25	Figure 52: System Preferences Screen	54
Figure 21: Utilities Menu	26	Figure 53: Transponder Comm Port Setup Screen	57
Figure 22: Backup Screen	26	Figure 54: Remote Port Setup Screen..	58
Figure 23: Restore Screen.....	27	Figure 55: Remote Setup Screen	59
Figure 24: Restore Warning Message Box.	27	Figure 56: Remote Connection Screen .	60
Figure 25: Restore Save Old database Message Box.....	28	Figure 57: Phone Book Edit Screen ...	61
Figure 26: Security Preferences Screen.	28	Figure 58: Pager Setup Screen	62
Figure 27: System Defaults Screen	31	Figure 59: Send Pager Message Screen	63
Figure 28: System Labels Screen.....	31	Figure 60: Printer menu	63
Figure 29: Print System Reports Screen.	31	Figure 61: Alarm Printer Screen	64
Figure 30: Alarm Report Generation Screen	32	Figure 62: Report Printer Screen	64
Figure 31: Schedule Screen	33	Figure 63: Print File Screen	64
Figure 32: Holiday selection in the Schedule Screen.....	33	Figure 64: Common Open File Screen ..	65
		Figure 65: Network Menu	65
		Figure 66: System Directories and Network Address Screen	65
		Figure 67: Current Network Socket Status Screen	67
		Figure 68: Winsock Data Screen	68
		Figure 69: This Computer's Name and IP Address Screen	68
		Figure 70: About Menu	68
		Figure 71: About Screen	69
		Figure 72: Remote Setup Screen	73
		Figure 73: Pager Setup Screen	74

Figure 74: Subscriber Database Advanced Screen	74
Figure 75: Transponder Area Edit Screen	75
Figure 76: Send a Pager Text Message Screen	75

Tables

Table 1: Importing a Subscriber Database	77
---	----

1.0 Security Escort System Architecture

1.1 System Components

1.1.1 System Overview

The Security Escort System consists of five basic components: transmitters, receivers, alert units, transponders, and the central console.

The transmitter is a miniature, radio transmitter, used to transmit either a distress or a test signal. The receivers are located throughout a protected area and detect the radio transmissions from transmitters. Alert units are siren/strobe units activated in the event of an alarm. Transponders are devices that control groups of receivers and alert units, connected to them by wire. Each transponder relays alarm and test signals from its receivers to the central console. In addition, the transponder tests for device and wiring faults, and transmits problem conditions to the central console. The central console consists of a computer (the master computer), an optional backup computer (the slave computer). Up to eight optional workstation computers can be used to receive alarm and trouble signals from the transponders, analyze the signals, activate strobes and sirens on the alert units, and produce a display for the security dispatcher. Each of these system elements is described more fully below.

1.1.2 Transmitter

There are several types of transmitters for personal use; those normally assigned to system subscribers, one for security personnel, and one for maintenance personnel. Each transmitter type serves a different purpose. All versions of transmitters for personal use produce alarm and test transmissions.

Subscriber Transmitter

Each transmitter contains a unique code, which is associated with the subscriber at the time the transmitter is assigned. In the event of an emergency, press and hold the alarm button(s) for 1 sec. to produce an alarm (see your transmitter user manual). Optionally, within approximately 2 sec., the sounders in a

nearby receiver activate, as well as the strobes and sirens on nearby alert units.

The transmitters have a second feature, the test mode. When the user is indoors, in sight of an interior receiver or outdoors, in sight of an alert unit, pressing the test sequence performs a test (see your transmitter *User's Manual*). If the test is successful, a small green light flashes on the interior receiver, or the strobe on an alert unit flashes briefly. There is no response at all if the test fails. If the test fails, the user should try again. If there is still no response, the user should contact the security office as soon as possible. Every successful test is recorded in the Subscriber Database in the central console software and optionally printed on the hardcopy printer. The Subscriber Database contains all of the information relating to each subscriber, including the date and time of the most recent test transmission. It is possible to search the Subscriber Database for individuals who have not performed tests for a specified period of time.

Security Transmitter

The Security Transmitters are unique in the way that both tests and alarms are processed. Outwardly, Security Transmitters perform in the same manner as normal transmitters during testing. That is, strobes flash on alert units and green lights flash on receivers to confirm a successful test. However, when a Security Transmitter is tested within close proximity of a receiver, the central console records not only the user identity, and the date and time (as with a normal user test) but also the location of the officer at the time of the test. These tests are designated by the term security test on the printout at the central console and provide a convenient means of recording security patrols. (To protect user privacy, location information is not printed out for regular subscribers during tests.)

The Security Transmitters also differ in the way that alarms are managed. Unlike regular transmitters, no sound is emitted from the transmitter itself, no horns are activated on receivers, and no strobes or sirens are activated.

The console in the security office sounds an alert tone and displays the alarm as usual except for a yellow background and text advising that the event is a silent alarm from a security officer. This allows security personnel to call for assistance without attracting unwanted attention.

Maintenance Transmitter

The Maintenance Transmitter is used exclusively for system set-up and diagnosis. Maintenance alarms are used during the system set-up to verify that a receiver is functioning and is properly identified in the Transponder Database. The maintenance alarm is also used to measure the received signal strength of the receivers from any location within the protected area. The central console distinguishes the Maintenance Transmitter by its unique coded message and produces a printout of the signal strengths reported by receivers on each transponder.

In the Test Mode, the Maintenance Transmitter behaves like a normal Subscriber Transmitter except that the central console does not verify the user ID portion of the transmitted code. Unlike the Subscriber Transmitters, all Maintenance Transmitters are assumed to be valid.

Point Transmitter

The Point Transmitter is used to protect assets not people. It has a magnetic reed switch and a supervised loop that reports both open and shorted states. The software can be programmed to report alarms and troubles on any of these conditions going off normal with unique text identifying the condition. These transmitters are supervised and also optionally support the alarm follower.

1.1.3 Receiver

The receivers are located throughout the protected area, including building interiors. Inside buildings, the spacing of these devices depends on the building construction and the locating precision required. Outdoors, spacing depends on terrain and foliage conditions and building obstructions. The procedure for location of receivers is contained in *The Security Escort Installation Guide*.

Each receiver contains a radio receiver to detect the transmissions from transmitters, and microcomputers to decode and interpret the received test and alarm messages. In addition, the microcomputers monitor to detect tampering, and report such conditions to the transponder.

Each receiver contains a sounder similar to those in self-contained smoke detectors. These sounders are optionally activated if the receiver has detected an alarm transmission.

Indoor receivers are typically mounted on inside walls. They are housed in small beige, rectangular units. Indoor receivers have one red and one green light. The green light is used to indicate a successful test of a transmitter. The red light is only illuminated during certain system tests and during alarms.

Outdoor receivers are contained in small weatherproof boxes typically mounted on the sides of buildings and on light posts. Outdoor receivers do not have the visible red and green LED's. Outdoors, the strobe lights on the alert units flash to acknowledge successful tests.

In addition to its radio receiver, each receiver also contains a transmitter functionally similar to the hand held transmitters. This transmitter can be commanded by the central console to transmit a test message to other nearby receivers. This buddy checking is performed periodically to verify that the receiver sections of all receiver units are functioning satisfactorily.

1.1.4 Alert Unit

An alert unit consists of two components, a self-contained strobe/siren unit and an electronic driver unit. The latter may be housed in either a metal indoor enclosure or an outdoor enclosure (similar to the outdoor receiver enclosure), depending on the application. The strobe siren units are always mounted in outdoor locations. In addition to the function of attracting attention in the event of an emergency, the strobe unit is used to acknowledge a successful test of a transmitter.

The alert unit has back-up battery power in addition to AC power. The alert unit driver contains a microprocessor, which communicates with the transponder for strobe and siren commands, status reports, and trouble indications. The troubles monitored are tamper, loss of AC power, and low battery.

1.1.5 Transponder

The transponder is a device controller for up to 64 devices; any combination of receivers and alert units. The devices are connected to the transponder by means of 8 four wire multiplex busses, two wires for power and two wires for data. Each bus is capable of supporting up to eight devices. The Security Escort System supports up to 255 transponders.

Each receiver and alert unit is identified to its transponder by a multiplex address that is set during system installation using a multi-position switch on the receiver or alert unit circuit board. Transponders communicate on the data bus with individual multiplex devices by issuing commands, which contain the receiver or alert unit's multiplex address. Note that a given transponder may have up to eight devices with the same binary multiplex address, one on each bus. Thus, the complete identification of a particular device must include the transponder with which it is associated (1 to 255), the bus on which it is located (0 to 7), and its binary multiplex address (0 to 7).

When a receiver or alert unit detects a reportable event (alarm, test, tamper, loss of AC power, and so on) it goes into an Off Normal state. To quickly locate any devices which might be in the Off Normal state, global commands (which are interpreted simultaneously by all of its devices) are issued by the transponder approximately ten times per second. These global commands are followed by commands to specific devices to determine the nature of the Off Normal condition and, in the case of an alarm or test, to obtain the Transmitter Identification Number, Transmitter Battery Condition, and Received Signal Strength. This information is used by the central console to identify the subscriber transmitting the alarm (test) and to determine the subscriber's location.

1.1.6 Central Console

The central console consists of one to eight IBM™ PC compatible computers running the Security Escort software within the Microsoft Windows environment. One computer serves as the main controller for the entire Security Escort System (the master computer) and a second serves as an optional backup (the slave computer). The other computers serve as workstations for the operators of the software. The slave and workstation computers can be used for administrative functions such as adding subscribers or performing routine system tests without interfering with the operation of the master computer.

In the event of an alarm from a transmitter, the console displays the name of the individual to whom the transmitter is assigned, and the location from which the transmission was made. The location information is shown graphically on a map of the protected area. Other information about the subscriber, such as address, home address, phone number, and any disabilities may also be shown.

Both the main computer and the backup record all messages sent between the central console and the transponders, providing redundancy of records.

1.1.7 Software Overview

The central console contains all of the operating software and all of the databases required by the Security Escort System. The *Security Escort System Operations Manual* describes that portion of the system software, which affects system operators (in most cases, the Security Department personnel). This *Technical Manual* discusses only the software functions that are specific to installation and maintenance of the system.

All operations on the central console computers are password access controlled. The **Logout** option on the **Main Menu** bar produces a screen for entry of the password (see *Figure 1*). Passwords may have different authority levels, assigned by installation company personnel or the Security Department's key operator.

Figure 1: Screen Box for Password Entry



Operations not accessible at a given authority level appear in gray rather than black on the central console. The installation and maintenance portion of the Security Escort Software is designed to facilitate set-up and modification of the system and to provide rapid diagnosis of system problems, usually with only one person being required. From the central console, simple commands can be used to scan all devices on a particular transponder for their current status. Devices can be enabled or disabled from the central console and the on-board transmitter of one receiver can be activated to test an adjacent receiver in order to confirm that its radio receiver section is operating properly (buddy check).

The Security Escort Software also continually monitors the status of each transponder to insure it is functioning correctly. All communications between the central console and a transponder require acknowledgments to verify message integrity. Each transponder must transmit a message periodically, to assure the central console that the transponder is still operating properly. Should a transponder fail to transmit either a routine status report or any other message to the central console, the central console sends a query to the transponder requesting a message be returned. If there is no response after six attempts at communications, a pop-up alert appears on the central console.

1.2 System Operation

The following sections describe the basic operation of the Security Escort System during alarm, test, and various other routine and emergency situations.

1.2.1 Alarm Sequence

Transmitter

When a user of the Security Escort System activates an alarm with the transmitter, multiple identical packets of digital data are transmitted from the hand-held transmitter to nearby receivers. Each packet contains a unique device identification code, an alarm type indication, the transmitter battery condition, and a check sequence. Multiple packets are employed to assure successful receipt of the message by the receivers.

Receiver

The receiver is continuously listening for radio signals that might be alarm or test data from transmitters. If the incoming message is determined to be valid, representing either an alarm or a test from a transmitter, the peak amplitude of the received signal is recorded.

Transponder Scanning

The transponder continually scans all of its receivers to see if any of them received a valid transmission. Once a transponder determines that one or more of its receivers received a transmission, it directs a message to those receivers, to determine the specifics of the transmission.

Receiver's Response

The receivers respond to these messages with the identification code of the transmitter that sent the alarm or test, the alarm or test type, and the amplitude of the signal received from the transmitter.

Transponder Data Collection and Response

The transponder next constructs a message for the central console containing the receiver addresses, for all receivers responding to the event and signal levels of the receptions, the alarm or test type and the transmitter identification number. The transponder then verifies that the communications channel is free and transmits the information to the central console. If the communication channel is busy, the transponder delays a random period of time and tries again.

Central Console Response

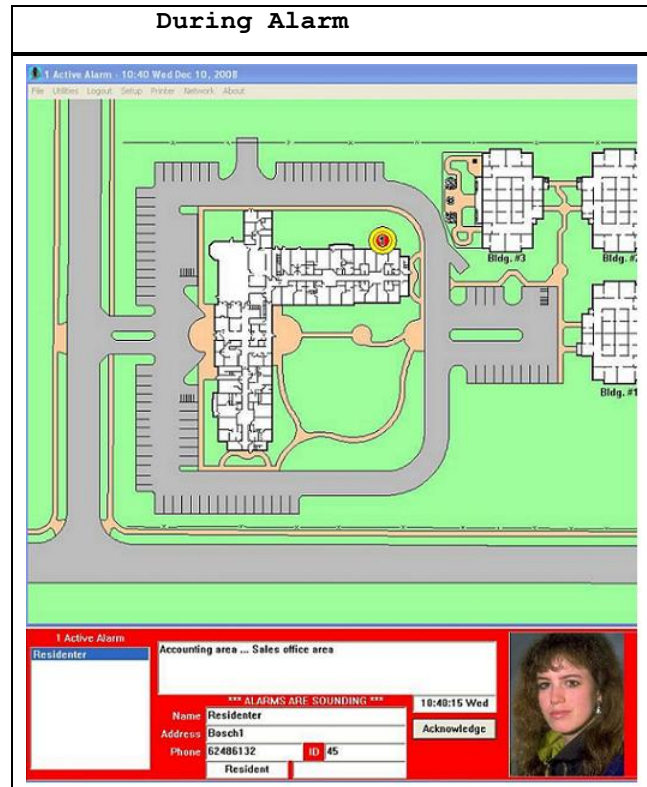
After acknowledging the alarm transmission from the first transponder, the central console begins its alarm analysis while collecting the alarm data from all other transponders, which had receivers that detected the alarm. The Subscriber Database is checked to determine the appropriate reaction to the alarm. If the transmitter is assigned to a valid subscriber and it is not designated as a security or watchman device, the central console commands the transponders to turn on the appropriate alert units. Depending on the settings selected in the **Security Preferences Screen**, this enables only the strobe portion of the alert unit, or both the strobe and siren. If the transmitter is unassigned, or has been disabled by selection of that option in the Subscriber Database, no commands will be issued to activate the alert units.

Note:

An option in the Security Preferences Screen allows unauthorized transmitters (not programmed in the database) to be treated like authorized transmitters. For example, strobes and/or sirens can be activated in the case of an alarm transmission (if they are also set to be activated for authorized transmitters).

The central console computes the location of the transmitter by comparing the signal strengths measured by the receivers which detected the transmission.

A partial map of the protected area is displayed on the central console, centered on the computed location, and a yellow circle is drawn to assist the operator in guiding the response personnel to the probable source of the transmission. Other data drawn from the Subscriber Database is added to the central console display to assist in the response to the alarm. In addition, the central console enunciator is activated to alert the operator to the event.



The central console also writes the time, location, and identity information to the hardcopy printer and writes a complete record of all activities to the hard disks on both the primary and backup computers.

Operator's Response

The operator reacts to the alarm by acknowledging the event with a keystroke or click of the mouse, which silences the alert sound from the central console. This silences only the central console enunciator, not the outdoor sirens or interior horns. The operator then directs response personnel to the scene and awaits their indication that the problem was resolved.

When the response personnel advise the operator that the problem is under control, the operator enters his password into a box on the central console. This step causes the central console to send commands to the transponders to silence the sirens and horns and extinguish the strobes and LED's. A reset of the system is accomplished with another key stroke or a mouse click on the **Reset** button on the screen.

Figure 2: Central Console Screen

Multiple Alarms

Receivers can handle multiple separate alarm or test events at the same time. If the receiver's event buffer is full but contains test events, it discards the test records in favor of an incoming alarm. Similarly, the transponder event buffer can hold multiple events and it also replaces test events with alarm events when its buffer is full.

To assure that simultaneous alarms are detected, the multiple identical packets sent by the transmitters are randomly spaced over approximately one second. Only one of the packets must be detected to produce an alarm. Thus a collision between the transmissions of two or more transmitters is virtually eliminated. In addition, unless the transmitters are in the same location, they detect different groups of receivers. The central console is capable of processing 30 concurrent alarms. When there is more than one active alarm, the central console displays data for the first to be received and also indicates the total number received and the identity of the individuals transmitting them. The operator can click on the name of an individual to see the data for a particular alarm.

1.2.2 Test Sequence

Transmitter

When the user of the Security Escort System activates a test transmission, multiple identical packets of digital data are transmitted. In this case, the digital data in the transmitted packets contain a test code rather than an alarm code.

Receiver

The receiver responds to a test transmission the same as to an alarm transmission by decoding the radio signals, and measuring signal levels.

Transponder Data Collection and Response

The transponder collects data on a test event in the same manner as for an alarm event, it does not command the LED (green for test confirmation) to flash until it has been commanded to do so by the central console. Transmitters not in the Subscriber Database, or in

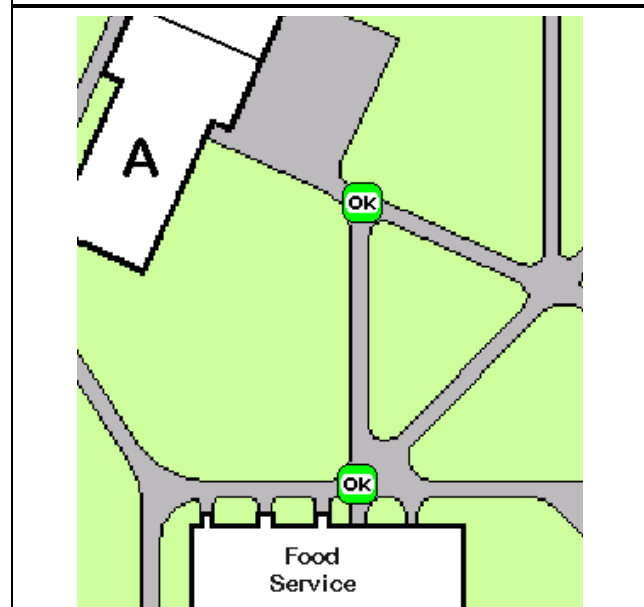
the database, but disabled, do not receive a flashing green light or flashing strobe that would indicate a successful test.

Central Console Response

The central console responds to the report of a test from a transmitter by collecting the data from each transponder reporting the event, and recording the locations of the receivers that detected the transmission. In this case, however, it does not calculate a location estimate. It simply records the data on the primary and backup computers' hard disks, prints the identity of the subscriber, date and time on the hardcopy printout, and displays generic test icons on the central console in positions corresponding to the locations of receivers hearing the transmission.

In the case of test transmissions from Security Transmitters or Watchman Transmitters, the central console determines the closest receiver to the transmission and creates a guard tour event which becomes a part of the Guard Tour Report.

Figure 3: Console Screen Showing test Icons



Operator's Response

There is no response required of the operator in the case of a test transmission.

2.0 Setting Up The System

2.1 Initial System Configuration

The default password is PPP. The default password, the Master password, and passwords for all system operators added by referring to the Operators Database in the *Security Escort Operations Manual* should be changed.

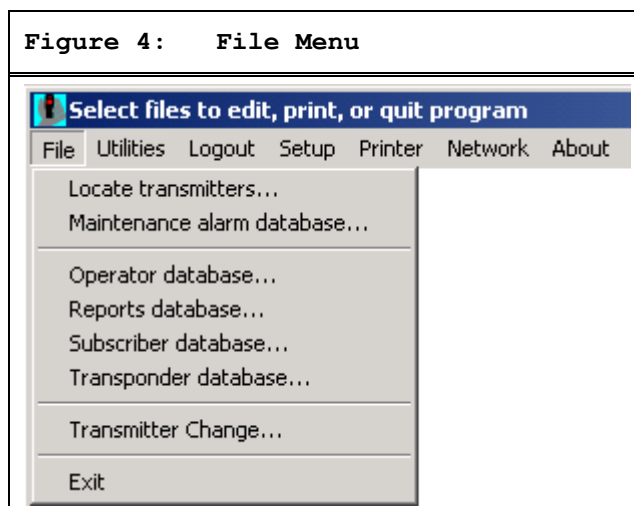
- To generate the map file for the screen display, refer to *Section 5.1 Map File Generation and Scaling*.
- To setup the transponder COMM ports refer to the *Section 3.3.18 Transponder Comm Port Setup Screen*.
- To setup the system COMM ports refer to the *Section 3.3.19 Remote Comm Port Setup Screen*.
- To set the function of the system COMM ports and setup remote access, see *Section 3.3.20 Remote Setup Screen*.
- To program the system configuration, see *Section 3.1.6 Transponder Database*.
- To program the system responses to an alarm, see *Section 3.2.3 Security Preferences Screen*.
- To program the system responses to troubles, see *Section 3.3.3 Popup Trouble Filter*.
- After communications to the transponders are established for any transponder that uses a Proxim Radio to communicate, program the **Uses Proxim Radio** field in the Transponder Parameter Change Screen. If all alarms are to be silent, program the **Run Silent** field. (See *Section 3.3.11 Transponder Parameter Change Screen*.)
- If this system has master and slave computers, set the Default Master Computer and Default Slave Computer. (See *Section 3.3.20 Remote Setup Screen*.)
- If using pager access in this system, see *Section 3.3.23 Pager Setup Screen*.

- If this computer runs other programs at the same time, Security Escort is running, set the **Not Always Top Window** field (see *Section 3.2.3 Security Preferences Screen*).
- To program the ID Receiver to automatically enter the transmitter IDs, see *Section 3.2.3 Security Preferences Screen*.
- To set the names of the subscriber classes, see System Default Screen in the *Security Escort Operations Manual*.
- To program the transmitters into the Subscriber Database, refer to the *Security Escort Operations Manual*.

3.0 System Menus and Screens

3.1 File Menu

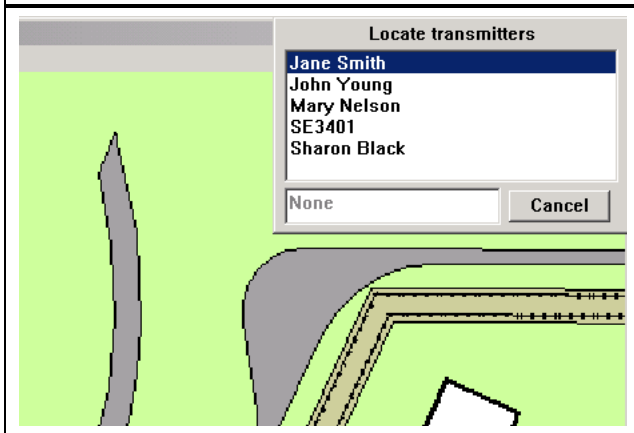
Figure 4: File Menu



3.1.1 Locate Transmitters

This selection allows the operator to display the last reported location of the transmitter assigned to the indicated individual or asset. When the individual or asset is selected from the list, the time of the last supervision report is shown (or None is displayed if no supervision report was received from that transmitter). On the map, the last report location is shown.

Figure 5: Locate Transmitters



3.1.2 Maintenance Alarm Database

Maintenance Transmitters, when activated in the Test or Alarm Mode, generate a series of multiple data packets like Subscriber Transmitters, however, a special code in each packet identifies the transmitter as a Maintenance Transmitter.

The receiver responds to a maintenance alarm or test transmission in the same way it responds to a subscriber alarm or test, unless the receiver is put in the Setup Mode. The transponder then reports the Maintenance Transmitter identification number and all signal levels to the central console which creates the location estimate and processes the data as it would for a normal alarm.

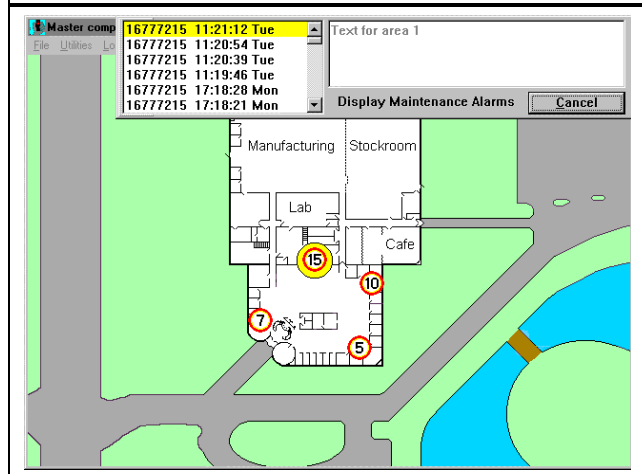
Note:

All Maintenance Transmitters are assumed to be valid so there is no need for the central console to check for the identification number in the Subscriber Database.

The central console does not generate an audible alert for the operator and does not create an alarm display on the main central console. Because they can be set to graphically display received signal levels, maintenance alarms are very useful in verifying that the system coverage exists at any location in the protected area and that receiver redundancy is adequate.

Figure 6: Maintenance alarm with

Signal Levels Shown in Icons"



3.1.3 Operator Database

The Operator Database contains the information on the individuals who are authorized to operate the system, their authority levels, and passwords. See the *Security Escort Operations Manual*.

3.1.4 Reports Database

The Reports Database contains the information on alarms that were previously processed by the system. Alarm data and maps showing the operators view can be recalled. See the *Security Escort Operations Manual*.

3.1.5 Subscriber Database

The Subscriber Database contains the information on the transmitters that are assigned in the system. See the *Security Escort Operations Manual*. When the **Advanced** button is pressed in the Subscriber Database Edit Screen, the Edit Subscriber's Advanced Features Screen (Figure 7) displays.

The Edit Subscriber's Advanced Features Screen is used to set up special transmitters that monitor fixed locations, subscriber pager access, parameters for point transmitters, the virtual fence for a wandering alarm, the alarm group for arming of the transmitter, and check-in requirements for this transmitter.

Figure 7: Edit Subscriber's Advanced Features Screen

Phone Number

This phone number is dialed to send a pager message to this subscriber. Typically, this is a different phone number than the one that is manually dialed to access this pager. The phone number is assigned by the paging service.

Pager Password

This is the password to be sent to the paging service when a page is sent to this subscriber. Leave blank if not required (typically the pager password is not required). The pager password is assigned by the paging service.

Pager ID

This is the ID that identifies the pager to receive the pager message (many times this value is the last seven digits that are manually dialed to access this pager). The pager ID is assigned by the paging service.

Pager Group

These are the pager groups that this subscriber is a member of. This subscriber can be a member of up to three different pager groups.

Pager Confirmation Not Required

If checked, the confirmation pager message is not sent to this pager if alarm is acknowledged by an acknowledgement transmitter.

Fixed Location Transmitter

This section is used only when this transmitter is mounted in a fixed location (it does not move). When this transmitter transmits an alarm, it is always reported at the programmed location.

Floor Level

This is the floor level where this alarm is located for a fixed location transmitter.

Map X Position

This is the X coordinate of the map position where this alarm is located for a fixed location transmitter.

Map Y Position

This is the Y coordinate of the map position where this alarm is located for a fixed location transmitter.

Locate

When clicked, the Edit Subscriber's Advanced Features Screen disappears and the cursor changes to a cross hair. Moving the cursor to a point on the map and clicking the left mouse button scrolls the map to that point at the center of the screen.

When the map is showing the desired alarm location, move the cross hair to the exact location of the alarm to be reported and click the right mouse button. The Edit Subscriber's Advanced Features Screen reappears and the selected location is entered into the X and Y coordinates.

If while the cross hair cursor is displayed, you want to exit without changing any coordinate values, press the [ESC] key and the Edit Subscriber's Advanced Features Screen reappears.

Map Number

Defines which bitmap is displayed for the fixed location of this transmitter. The default map is zero, which corresponds to bitmap MAP0.EDB stored in the Escort sub-directory. Map 1 would be MAP1.EDB. There can be 100 maps per Security Escort System (0 to 99).

Enable Reed Switch

If checked, the reed switch input of this transmitter is enabled and causes an alarm. Otherwise, the reed switch input is disabled. The alarm group this transmitter is assigned to must be armed, for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. To enable this option, the transmitter's class must be set to point type.

Optional Text

This is optional text that can be added to the location text when this input reports an alarm. To enable this option, the transmitter's class must be set to point type.

Disable Shorted Loop

If selected, a shorted loop on this transmitter does not cause an alarm or trouble report to display. To enable this option, the transmitter's class must be set to point type.

Alarm on Shorted Loop

If selected and the alarm group this transmitter is assigned to is armed, a shorted loop on this transmitter causes an Alarm Report to display. For this input to cause an alarm, the alarm group this transmitter is assigned to must be armed, which is displayed. If no alarm group is assigned, the transmitter is always armed. To enable this option, the transmitter's class must be set to point type.

Trouble on Shorted Loop

If selected, a shorted loop on this transmitter causes a Trouble Report to display. To enable this option, the transmitter's class must be set to point type.

Alarm When Armed, Trouble When Disarmed on Shorted Loop

If selected and the alarm group this transmitter is assigned to is armed, a shorted loop on this transmitter causes an Alarm Report to display. If selected and the alarm group this transmitter is assigned to is disarmed, then a shorted loop on this transmitter causes a Trouble Report to display. If no alarm group is assigned, the transmitter is always armed. To enable this option, the transmitter's class must be set to point type.

Disable Open Loop

If selected, an open loop on this transmitter does not cause an Alarm or Trouble Report to display. To enable this option, the transmitter's class must be set to point type.

Alarm on Open Loop

If selected and the alarm group this transmitter is assigned to is armed, an open loop on this transmitter causes an Alarm Report to display. The alarm group this transmitter is assigned to must be armed for this input to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed. To enable this option, the transmitter's class must be set to point type.

Trouble on Open Loop

If selected, an open loop on this transmitter causes a Trouble Report to display. To enable this option, the transmitter's class must be set to point type.

Alarm When Armed, Trouble When Disarmed on Open Loop

If selected and the alarm group this transmitter is assigned to is armed, an open loop on this transmitter causes an Alarm Report to display. If selected and the alarm group this transmitter is assigned to is disarmed, an open loop on this transmitter causes a Trouble Report to display. If no alarm group is assigned, the transmitter is always armed. To enable this option, the transmitter's class must be set to point type.

Fixed Location and Pager Text

This is the text that displays as the location of the alarm for fixed location transmitters and on pagers reporting this alarm.

Transponder Name

Select the transponder with the area that defines the area for a wandering (virtual fence) alarm. Refer to Transponder Area for the operation and setup of the wandering alarm (virtual fence alarm).

Transponder Area

Wandering Alarm - Create a protected area by placing a virtual monitor fence around an area of the main map. These areas are defined in the transponder database. If this transmitter is constrained to remain within one of these defined areas, first select the defining transponder in the **Transponder Name** field. Then select the desired area from this dropdown list of the transponder's area names.

For the wandering alarm to work, the supervision period must also be programmed for this transmitter.

Specific transmitters are marked in the Subscriber Database to be constrained within a specific fenced area defined by this option. If the transmitters leave their defined area, the system reports this as a wandering alarm and continues to monitor and track the location of the transmitter until the alarm is canceled from the screen in the normal way. However, these tracking updates can only occur every supervision transmission period (not on an accelerated rate like a tracking alarm).

The Security Escort System computes the location of the transmitters when they broadcast automatic supervision transmissions periodically.

Because of the basic location accuracy and the floor-to-floor accuracy of the system, there is a potential for some false alarms. If false alarms are a problem, check the **Filter Virtual Fence** checkbox in the Edit Security Preferences Screen. If you do this, two successive location calculations indicate the transmitter moved outside the protected area before an alarm was generated. The downside of this is a delay in the reporting of a wandering alarm of one extra transmitter supervision period.

Alarm Group

This is the alarm group that controls the arm/disarm status of this transmitter. Select the desired alarm group from the dropdown list. This alarm group must be armed for this transmitter to cause an alarm, which is displayed. If no alarm group is assigned, the transmitter is always armed.

Requires Check-in

When this checkbox is checked, this transmitter activates once each day during the check-in schedule time. At the end of the check-in period, if the subscriber fails to check-in, a Failed to Check-in Report is generated and presented to the operator. This report contains all of the people who failed to check-in with their first address line and phone number. All subscribers in the report must be checked on to make sure they are not in need of assistance, as this may be a life-threatening situation. A printed report may be generated.

If the transmitter is not a point type, the transmitter can generate alarms and therefore a test transmission is used for the check-in.

If the transmitter is a point type, any non-trouble transmission serves as a check-in.

One of the ten schedules must be selected as the check-in schedule to define the check-in period.

Done

Click this button when all changes are complete to return the main Subscriber Database Edit Screen.

3.1.6 Transponder Database

The Transponder Database is established at system set-up and contains all necessary configuration data for each transponder, receiver, and alert unit. It describes the basic structure of the installation, including all device names, locations, types, multiplex addresses, and so on. This information is used by the central console to generate alarm and test displays on the central console and in determining which alert units are activated.

Figure 8: Find Transponder's

Database Record

Find Transponder's Database Record

Transponder Data Record size 6004 bytes, version 7

Transponder Created

Transponder ID Modified

Comm Port Index Radio ID Modify Oper

Isolate From All Other Transponders For Location Ignore Communications Failure

MUX Point Data

Point Number	Point Type	Transponder	Point
0	Receiver	Alert 1	
Bus 0, point 0	Bus + Bus -	Alert 2	
	Algorithm Default	Alert 3	
	Floor Level Floor 1	Test	

Location

SA% Map

Access the Transponder Database from the **File Menu** on the **Main Menu** bar. The following paragraphs describe the elements of the Find Transponder's Database Record Screen.

Transponder

This box contains the names of the transponders. Clicking the arrow to the right of this box displays a drop-down list. The names of each transponder in the system display, allowing easy selection for review or editing.

The transponder names are assigned during set-up and used to indicate the physical location of the transponder or the region of the protected area covered by a particular transponder.

Created, Modified, Modify Oper

The system software automatically creates these three fields to the right of the Find Transponder's Database Record Screen. They represent the date the transponder was first entered into the Transponder Database, the date of the last change of any entry for this transponder, and the identity of the operator who made the last change (determined from the password entered to make the change).

Transponder ID

This is a number assigned to the transponder at system set-up. It is used by the central console to identify the transponder during all communications between the central console and the transponder. The number must agree with the transponder address, which is set during final installation by switches on the transponder circuit board.

Note:

Zero is not allowed as a transponder address.

Comm Port Index

This indicates which central console communications port to use to communicate with this transponder. The Transponder Comm Port Setup Screen selects the specific physical port that this index refers.

Radio ID

This is the identification number for the radio interface unit, if the transponder communicates to the central console by a radio link. (This feature is currently not implemented.)

Isolate From All Other Transponders For Location

When checked, this transponder is isolated from all other transponders for location considerations. This is used when distant transponders sometimes hear an alarm and throw off the alarm location calculation. If this checkbox is checked, it indicates that this transponder is protecting an area that is independent of all other transponders in the system. When an alarm is reported and receivers on this transponder have the best reception, only the receivers on this transponder are considered for the location of this alarm. If another transponder has the best reception, then the receivers on this transponder are ignored for the location of this alarm.

Ignore Communications Failure

This checkbox allows communications failures to be ignored for this transponder. It is used during a new installation for transponders that are not yet fully on line. During system maintenance when a transponder is out of service for a while, it is used so that the communications failure messages do not flash on the screen and distract the operator. Checking this checkbox causes the system to ignore communication failure. Therefore, if communications fail with this transponder, the area this transponder protects is not protected and alarms from subscribers in that area are missed without the operator's knowledge. **This checkbox should not be checked in a live system.**

Insert New

Clicking this button displays a new Edit Subscriber's Advanced Features Screen. This is used to enter a new transponder to the database.

Edit Data

Clicking this button allows the currently displayed transponder's database record to be edited.

Kill Transponder

Clicking this button deletes the displayed transponder's database record. If the transponder is deleted, its data is permanently deleted and cannot be recovered.

Delete Point

Clicking this button deletes the displayed point only from the displayed transponder's database record. If the point is deleted, its data is permanently deleted and cannot be recovered.

Copy

Clicking this button copies the displayed transponder's database record into a new transponder record. This allows similarly configured transponders to be programmed once, then copied into a new record.

Note:

*It is not possible to edit the transponder ID itself. If this should be necessary, the **Copy** button can be used to produce another Transponder Database entry duplicating the first, but with the transponder ID blank. The new transponder ID can be entered, the new data saved by using the **Save** button, and the old transponder entry can be deleted by using the **Kill Transponder** button.*

Print

Clicking this button prints the displayed transponder's database record.

Beginning

Clicking this button changes the displayed transponder to the first transponder in the database.

Previous

Clicking this button changes the displayed transponder to the previous transponder in the database.

Next

Clicking this button changes the displayed transponder to the next transponder in the database.

End of File

Clicking this button changes the displayed transponder to the last transponder in the database.

Mux Point Data

The lower portion of the Find Transponder's Database Screen provides information on each of the devices controlled by the transponder selected in the **Transponder** field. Two digits represent each receiver or alert unit address; the first is the number of the multiplex bus on which the device is mounted (0 to 7) and the second is the multiplex point address assigned to the particular device. On each of the eight multiplex busses up to eight devices may be installed, but each device must be assigned a unique multiplex point address (0 to 7). More than one device can have a particular multiplex point address, but only if on different busses. The multiplex point addresses are assigned by switch settings on the device (receiver or alert unit) circuit boards. These multiplex point address settings are also a part of the Transponder Database. The multiplex address shown in the Transponder Database and the multiplex address set on the device circuit board must agree. The Transponder Setup Screen is used to verify multiplex address settings.



It is a good idea to create an entry in the Transponder Database for each transponder in the system before entering the data for each device so that all transponders appear in the drop-down menus.

3.1.7 Creating a New Transponder Entry

The creation and modification of the Transponder Database requires special authority levels usually assigned only to installation company personnel.

The **Insert New** button creates a new Transponder Database Screen, ready for entry of data.

The System Design Layout Sheets prepared in advance by the installation manager should contain the necessary information for assigning the transponder name and ID, the comm port or radio ID, as well as the names and multiplex addresses for all receivers and alert units connected to each transponder.

The System Design Layout Sheets also contain the text used to indicate the receiver locations and designates the alert units driven by each receiver.

Figure 9: Blank Screen Resulting from Selecting the Insert New Button

3.1.8 Setting Receiver Parameters

If the Transponder Database already contains the transponder, the **Edit** button is used to allow completion or modification of the data.

Trouble Type Text

This is the text that is shown in the Trouble Screen when the remote key input on the transponder goes active (shorted).

Trouble Tamper Text

This is the text that is shown in the Trouble Screen when the remote key input on the transponder goes into trouble (open).

Trouble Response Text

This is the text that is shown in the Trouble Screen as the response test. The actions the responding individual should take.

Show Points

If selected, the lower half of the Transponder Database's Screen shows the point's (receiver, virtual receiver, or alert unit's) database values.

Show Areas

If selected, the lower half of the Transponder Database's Screen shows the area's database values.

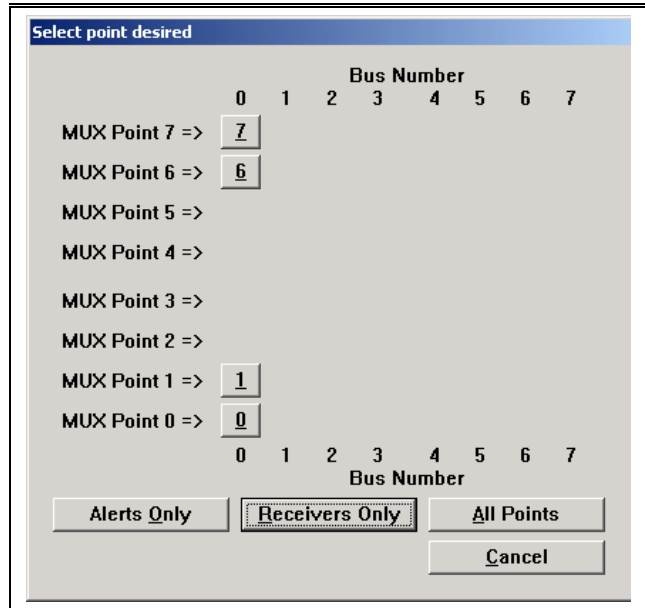
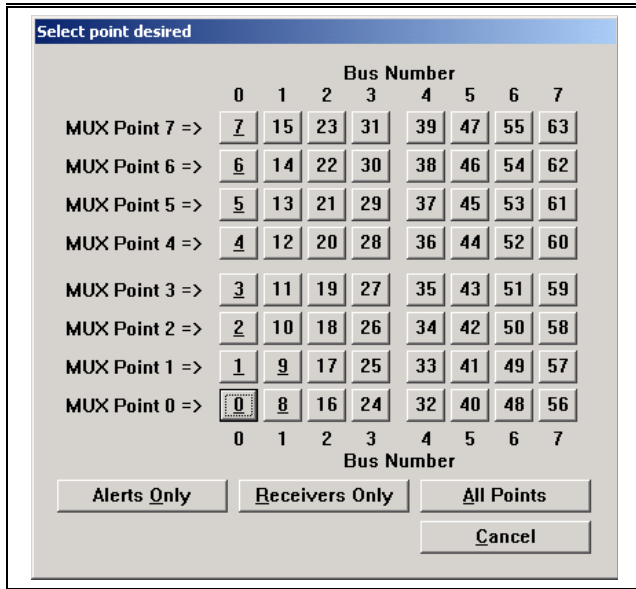
Area Number

Each Transponder can have up to 80 areas defined (prior to version 2.04 of the software only 40 areas could be defined). Area numbers range from 0 to 79. Use the **Locate** button to define the area graphically on the map.

Point Number

Each receiver and alert unit connected to the transponder has a unique point number assigned during the system design process. This number corresponds to a specific bus number and point multiplex address number. The multiplex address, set by means of switches on the device (receiver or alert unit) itself, must correspond with the point number assigned in the Transponder Database. For instance, a device programmed with multiplex address location 3 and on bus 5 is point number 29. This relationship is displayed in the table that displays anytime a ? box is clicked with the mouse. Clicking on any number in the table automatically enters that number into the **Point Number** field on the Transponder Database Screen and closes the table screen.

Figure 10: Select Point Screen with "All Points" Selected



A third number, the point number is unique to a particular device. Point numbers range from 0 to 63. There is a one-to-one correspondence between a point number and a point multiplex address/bus number pair. The point number assignment is presented in a table displayed whenever the ? box to the right of the **Point Number** field is clicked.

Figure 11 illustrates a quick way to select a particular device without having to translate between the two numbering systems. Three buttons at the bottom of this screen allow the user to display all possible device numbers (whether or not the particular transponder has a device assigned to the number) or, to display only locations populated by receivers or only locations populated by alert units.

When the **Point Number** button in the table is clicked, the Point Number table disappears and that point number automatically appears in the **Point Number** field of the Transponder Database Screen. The bus number and point address are also changed to reflect the selection

+, -, Bus + and Bus -

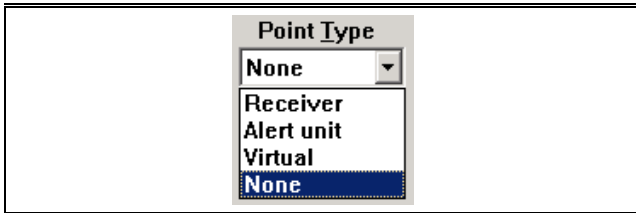
These buttons, just below the **Point Number** field, allow you to quickly advance the device selection by one location, either one point location (+ or -) or one bus number (Bus + or Bus -). This is useful when a task requires proceeding from device to device, as during system setup or check out. The ? box is used to display all devices to facilitate quick selection of a particular device. It is most useful when diagnosing a problem with a particular device.

Point Type

The **Point Type** field indicates the type of device (receiver, virtual receiver, or alert unit) located at the location currently selected in the **Point Number** field. Once the **Point Number** field contains the proper value, the device type is set by selecting from the options in the drop-down menu that appears when the arrow to the right of the **Point Type** field is clicked.

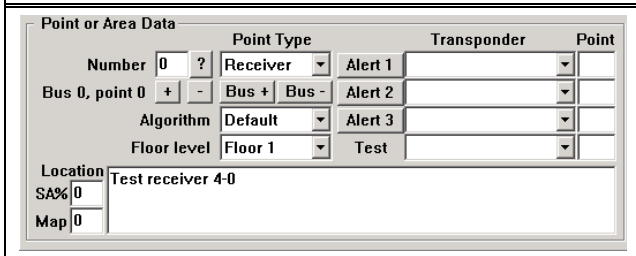
Figure 11: Select Point Screen with "Receivers Only" Selected

Figure 12: Drop-Down Menu for Selection of Point Type



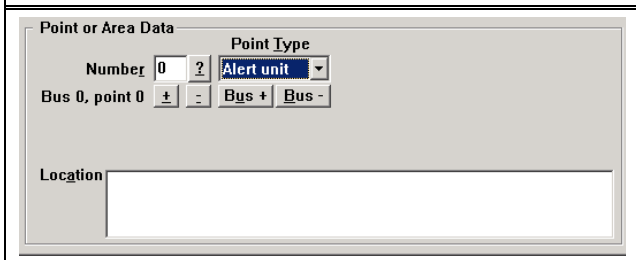
Use the receiver selection when there is a physical receiver connected at this bus location.

Figure 13: Data Entry After Selection of Receiver Point Type



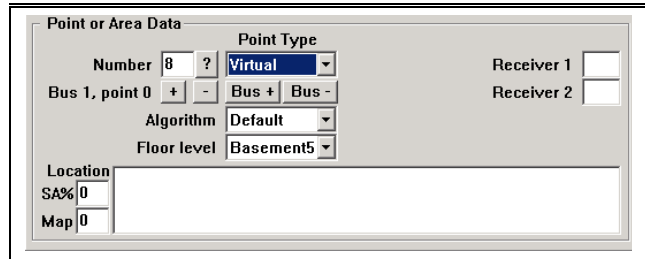
Use the alert unit selection when there is an alert unit connected at this bus location.

Figure 14: Data Entry after Selection of Alert Unit Point Type



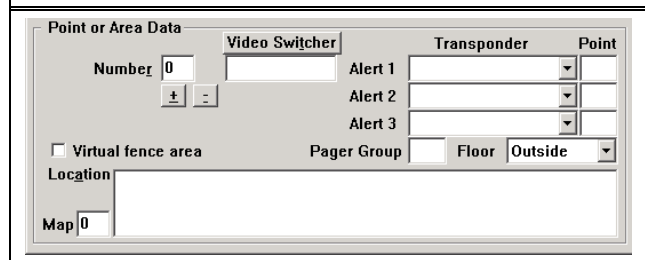
Use the virtual selection when there is no physical device connected at this bus location. Starting with version 2.03 of the Security Escort software, you can add virtual receivers in the Transponder Database. A virtual receiver is added at one of the 64 points allowed per transponder. However, there is no physical hardware used.

Figure 15: Data Entry after Selection of Virtual Receiver Point Type



The virtual receiver is intended to compensate in cases where there is a receiver imbalance. For example, if a building with a dense population of receivers is adjacent to a fence with few receivers and an alarm occurs between them, the alarm location can pull towards the building. The virtual receiver references two other physical receivers that must be on the same transponder. Only if both of the referenced receivers receive an alarm transmission, is the virtual receiver added to the alarm as if a physical receiver heard the alarm at the average receive level of the two referenced receivers. The virtual receiver's location and sensitivity can be adjusted the same as a physical receiver. After a virtual receiver is added, verify the surrounding areas to make sure they were not adversely affected. In no event, should a virtual receiver be utilized as a cost savings measure to avoid the installation of an actual receiver.

Figure 16: Data Entry when Show Areas is Selected



Alert 1, Alert 2, Alert 3, and Test

Each receiver can be assigned up to three alert units that are activated if it is one of the receivers reported by the transponder as part of an alarm event. Each receiver can also be assigned one alert unit that is activated to confirm test transmissions. These alert units do not need to be connected to the same transponder as the receiver. The **Transponder** field contains the transponder to which the designated alert unit is connected and the **Point** field contains the point number of the alert unit on that transponder.

The test boxes similarly designate the alert unit, if any, whose strobe unit is activated in the event of a test transmission from a transmitter.

To assign alert units to each receiver, use the drop-down menus to the right of the boxes labeled **Alert 1**, **Alert 2**, and **Alert 3** to select the transponder of the designated alert unit. Type point number into the **Point** field.

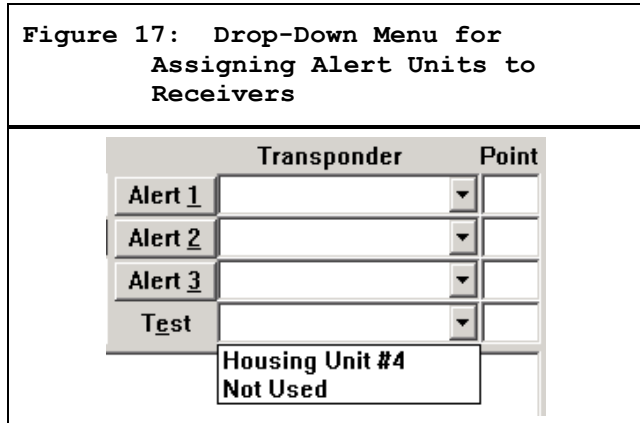
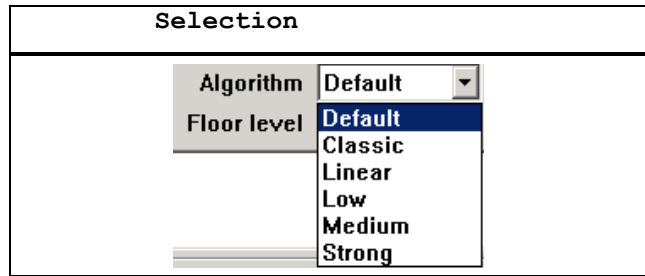


Figure 17: Drop-Down Menu for Assigning Alert Units to Receivers

Algorithm

Starting with version 2.03 of the Security Escort Software, there are five different location algorithms that can be selected on an individual receiver basis in the transponder database. Classic (original Escort algorithm), linear, low pull, medium pull, and strong pull. By default, when a receiver is set for outside or tunnel it uses the linear algorithm; all other receivers use the low pull algorithm. The receiver that hears the alarm transmission the strongest determines the algorithm used for this alarm.

Figure 18: Location Algorithm



Changing the algorithm setting for a receiver only affects the location when the alarm is close to this receiver and it hears the alarm the strongest. The stronger the pull the more the alarm is pulled towards the receiver, with linear having no extra pull.

The algorithm setting is only available if the **Enable algorithm tweaks** field is checked in the System Preferences Screen. Also Security Escort Software version 2.03 and higher, allows individual receiver sensitivity to be set in the Transponder Database. Receivers can be adjusted from 50% to 149% of their normal sensitivity using the **SA%** field.

Floor Level

This selects the physical floor level a receiver is mounted at or a virtual receiver acts like it is mounted at. It is very important that this setting is correct for the operation of the location algorithm.

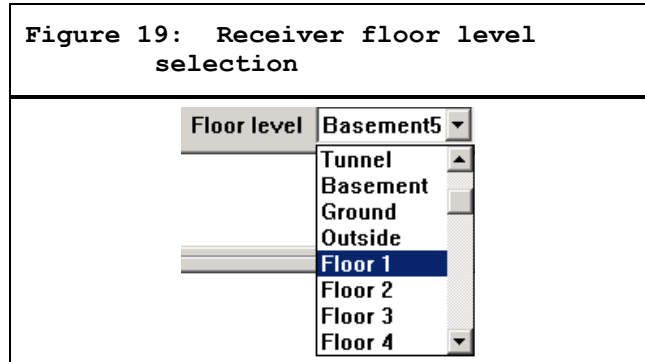


Figure 19: Receiver floor level selection

Receiver 1 and Receiver 2

These are the two receivers, on the same transponder, that a virtual receiver assumes the average of. Both receivers must receive a signal before the virtual receiver reports it also received a signal that is the average of the other two receivers signals. The location algorithm and sensitivity adjust work the same for a virtual receiver as for a physical receiver.

Location

This block contains the text to be displayed on the Alarm Screen if this receiver is one of those closest to the alarm source. The description is developed with the guidance of the security personnel who must respond to an alarm. It is vital that the description be clear and unambiguous to them.

To enter a location description, place the cursor in the **Location** field, click the mouse, and begin typing. Receiver and alert unit location names are important because they are used for directing response to an alarm and aid service personnel in identifying the device in the event of a problem. The Problem Reports displayed on the central console and printed by the hardcopy printer contain the device location descriptions that are entered in the **Location** field.

SA%

Security Escort Software version 2.03 and higher allow individual receiver sensitivity to be set in the Transponder Database. Receivers can be adjusted from 50% to 149% of their normal sensitivity. No physical receiver changes or upgrades are required. This setting should only be changed if there are known location accuracy problems in the area of this receiver. Settings of 50 to 99 desensitize the receiver to 50% to 99% of the actual received signal strength. Settings of 1 to 49 increase the sensitivity to 101% to 149% of the actual received signal strength. Try changing the sensitivity of receivers one at a time while testing the alarm location response. For example, if alarms are being pulled towards a particular receiver, lower its sensitivity in 10% increments and retest. If the area can be corrected using this method, verify the surrounding areas to make sure they have not been adversely affected. Generally, it is better if the correction is done in small steps while verifying the adjacent areas, rather than trying to correct the entire error in one step.

The SA% option is only available if the **Enable algorithm tweaks** field is checked in the System Preferences Screen. Also in the Transponder Database the **Algorithm** dropdown list allows selection of **Default, Classic, Linear, Low, Medium, or Strong** pull location algorithms for each transmitter. The point reporting the best reception level determines the actual algorithm used for the location on any event. If programmed for **Default**, the algorithm used is **Linear** for points programmed as outdoor or tunnel. All other points use **Low**. If the point reporting the best reception level is not programmed for the **Default** algorithm, the location calculation uses the algorithm programmed.

Map

Defines which bitmap to display for this receiver or area when an alarm is closest to it. The default map is 0, which corresponds to bitmap MAP0.EDB stored in the Security Escort sub-directory. Map 1 is MAP1.EDB. There can be 100 maps per Security Escort System (0 to 99).

Video Switcher

Selects a system serial port programmed in the Remote Setup Screen displaying the most likely area the alarm is located on the CCTV monitors near the central console. The string activates a macro in the video switcher that selects the appropriate camera and controls any required zoom and tilt actions. Up to 40 characters can be entered. Control characters can be entered as [^][A] for control A.

Pager Group

The pager group that is paged if the alarm location is determined to be in this area.

Floor

Determines the floor number that this area is defined for. The areas on floors above and below this one can be defined differently. For an area to be selected when an alarm is received, the location determined by the central console must be located within the defined area and must be located on the designated floor.

Virtual Fence Area

If this checkbox is checked, this area is not used for a normal alarm area location. This area is only used to define a virtual fence. Specific transmitters in the Subscriber Database can reference this transponder and area. When they reference this area and the system locates the transmitter position outside the area, a Wandering (Virtual Fence) Alarm is generated. This alerts the operator and shows the position of the transmitter.

Locate

When clicked, the Edit Transponder's Database Record Screen disappears and the cursor changes to a cross hair. Moving the cursor to a point on the map and clicking the left mouse button scrolls the map so the point is at the center of the screen and all previously defined receivers and areas are shown with numerical labels.

When the map is showing the location of the desired receiver, move the cross hair to the exact location of the receiver and click the right mouse button. The Edit Transponder's Database Record Screen reappears and the selected location is entered into the X and Y coordinates.

When the map shows the desired location, move the cross hair to the exact location of the first point of the polygon that describes the boundary of the area and right click. Move the cursor to the second point of the polygon and again right click. The computer draws a straight line between the first and second points. Repeat this process drawing all sides of the polygon to define the area. To close the polygon, place the last point on top of the first point. The polygon can have up to nineteen sides and no two lines of the polygon may cross each other. If you try to create more than nineteen sides, the computer automatically closes the polygon with the nineteenth side. When the polygon is closed, it can be crosshatched to make it more visible. After the polygon is complete, double click the left mouse button to return to the Edit Transponder's Database Record Screen.

If the area being defined is a virtual monitor "fence" area for Wandering Alarms, the monitor fence (area boundary) should be drawn at least 7.62 m (25 ft.) past the area to be protected to reduce potential false alarms.

If the cross hair cursor is displayed and you want to exit without changing any coordinate values, press the [ESC] key and the Edit Transponder's Database Record Screen reappears.

Cut

Clicking this button copies the displayed point or area data to a clipboard and returns all values to their defaults.

Copy

Clicking this button copies the displayed point or area data to a clipboard. Displayed values are not changed.

Paste

Clicking this button copies the clipboard values to the displayed point or area data. The values on the clipboard are not changed and can be copied to more points or areas.

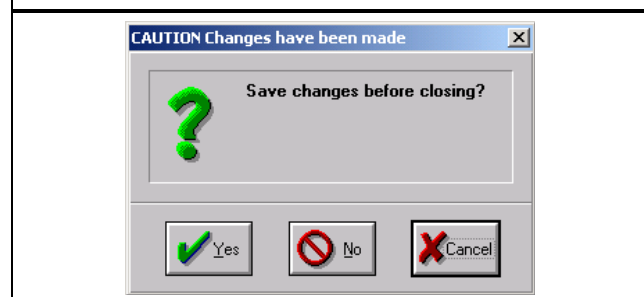
Save

Clicking this button saves all changes to the database.

Cancel

Clicking this button closes the screen. If changes were made, *Figure 20* displays giving you another chance to save the changes by clicking the **Yes** button.

Figure 20: Save Changes Screen Box



3

.1.9 Transmitter Change

Refer to the *Security Escort Operations Manual*.

3.1.10 Exit

Click this button to close the Security Escort application. Enter your password at the prompt to verify you have the authority to shut down the program.

3.2 Utilities Menu

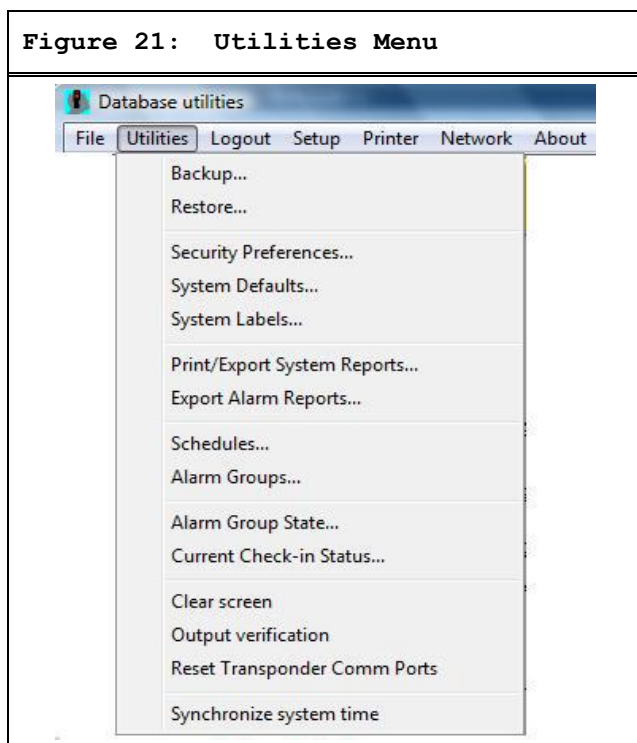
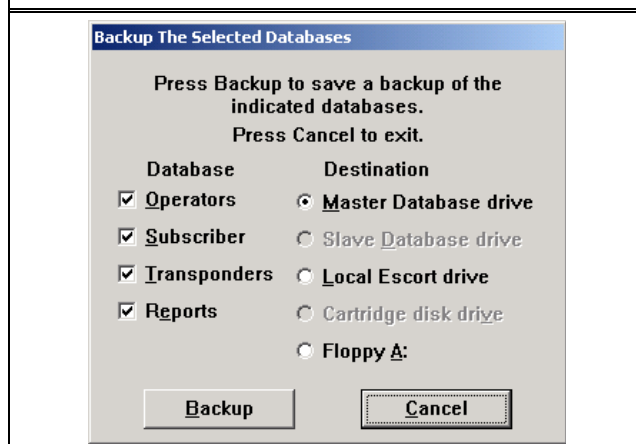


Figure 21: Utilities Menu

3.2.1 Backup Screen

Use this screen to make backups for all the databases. Only the databases with a checkmark are backed up. Preferably, all databases should be backed up at once. Only when they do not fit on one floppy should you save individual databases to one floppy; then switch floppy disks and repeat the procedure to save the rest of the files. As insurance against database problems, make multiple backups to different disks frequently. Store at least one backup copy in a different location from this system and remember to keep this copy current.

Figure 22: Backup Screen



Operators

This is the database of all individuals with passwords to operate the system software and acknowledge alarms.

Subscriber

This database contains all the transmitters assigned in the system.

Transponders

This database contains the transponders, receivers, virtual receivers, and alert units configurations.

Reports

This database contains all the Alarm Reports and related alarm map screens.

Master Database Drive

Store the backup files in the Security Escort Master Database path. See the System Directories and Network Address Screen.

Slave Database Drive

Store the backup files in the Security Escort Slave Database path. See the System Directories and Network Address Screen.

Local Database Drive

Store the backup files in the same sub-directory on this computer where the Security Escort System components are stored (typically C:\ESCORT).

Cartridge Disk Drive

Store the backup files in the **Backup/restore to disk cartridge path** field assigned in the System Preferences Screen. This path can point to a cartridge disk drive, a local hard disk, or a network disk drive.

Floppy A

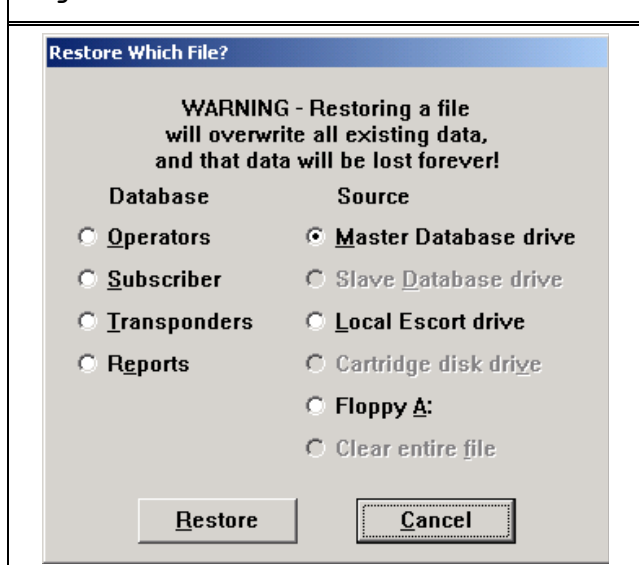
Store the backup files on the floppy disk in floppy disk drive A.

Backup

When the **Backup** button is clicked, all the databases selected with a checkmark are saved to the destination selected on the right.

3.2.2 Restore Screen

Use this screen to restore previously made database backups to the system databases. On the left, select the database to be restored. The right indicates where this database backup is currently located. Click the **Restore** button to replace the existing database file with the backup. This process also rebuilds the database and its index tables which corrects most database structure problems.

Figure 23: Restore Screen**Operators**

The database of all individuals with passwords to operate the system software and acknowledge alarms.

Subscriber

This database contains all transmitters assigned in the system.

Transponders

This database contains the transponders, receivers, virtual receivers, and alert units configurations.

Reports

This database contains all the alarm reports and related alarm map screens.

Master Database Drive

Store the backup files in the Security Escort Master Database directory. See the System Directories and Network Address Screen.

Slave Database Drive

Store the backup files in the Security Escort Slave Database directory. See the System Directories and Network Address Screen.

Local Database Drive

Store the backup files in the same sub-directory where on this computer the Security Escort System components are stored (typically C:\ESCORT).

Cartridge Disk Drive

Store the backup files in the **Backup/restore to disk cartridge path** field assigned in the System Preferences Screen. This path may point to a cartridge disk drive, a local hard disk, or a network disk drive.

Floppy A

Store the backup files on the floppy disk in floppy disk drive A.

Clear Entire File

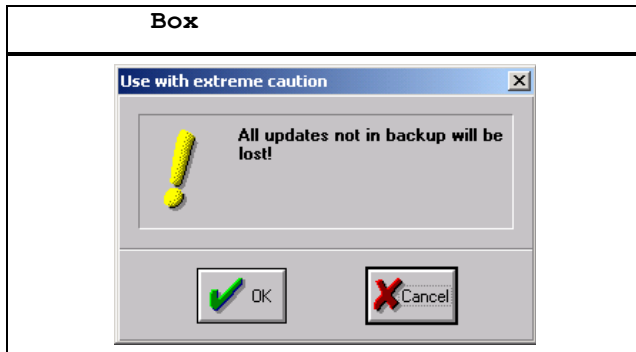
If the database is selected and the **Restore** button is clicked, the entire database is cleared of all records. **This selection must be used with extreme caution.** Hold down the [SHIFT] and [CTRL] keys when opening the screen to enable the **Clear Entire File** option.

Restore

When the **Restore** button is clicked, the database selected is restored from the destination selected on the right.

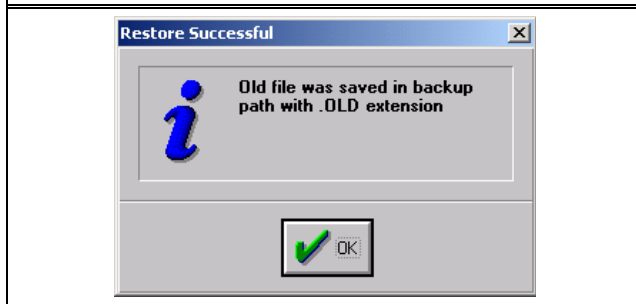
This message box is a reminder that if changes to the system databases were made since the backup was made, the changes are lost. Therefore those changes must be redone to the restored database.

Figure 24: Restore Warning Message



This message box indicates the restore was completed. The previous database file is renamed with an .OLD extension and saved in the Security Escort sub-directory. Only the most recent database of each type is retained.

Figure 25: Restore Save Old database Message Box



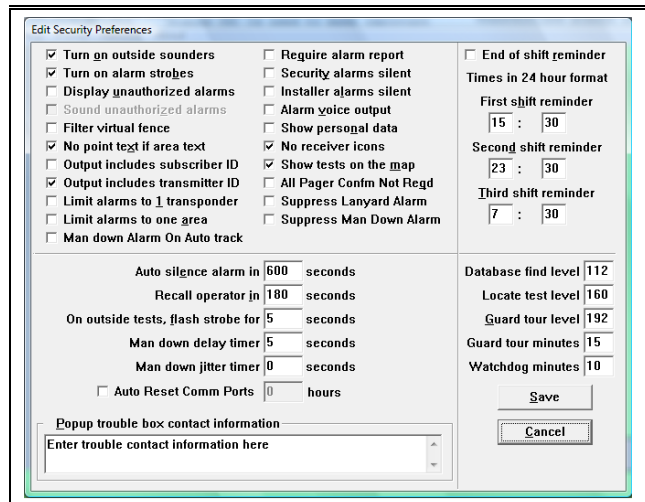
3.2.3 Security Preferences Screen

The Security Preferences Screen controls those aspects of the Security Escort System operation that are determined by the security director.

Turn On Outside Sounders

This checkbox is used to activate or deactivate the sirens on alert units and transponders. Some security directors prefer that all alarms be silent, others choose to employ sirens. Checking this option causes the sirens on the alert units to sound in the event of an alarm. Temporarily deactivating the sounders is necessary during maintenance.

Figure 26: Security Preferences Screen



Turn On Alarm Strobes

Checking this option causes the strobe lights on the alert units and transponders to flash in the event of an alarm.

Display Unauthorized Alarms

This checkbox determines if unauthorized alarms are displayed on the central console. Unauthorized alarms are those triggered by transmitters not currently registered in the Subscriber Database. These could be transmitters that were removed from the database because they were lost or stolen, transmitters not yet issued, or transmitters issued to subscribers at another Security Escort System. Typically, this checkbox should not be checked.

Sound Unauthorized Alarms

This checkbox determines if unauthorized alarms are to be sounded on the horns of the receivers and the sirens of the alert units and transponders. The option is not available unless the **Display Unauthorized Alarms** field is selected. Typically, this checkbox should not be checked.

Filter Virtual Fence

If the virtual fence option is used, check this box to reduce the number of the false alarms generated. If the box is checked, the actual alarms are delayed by the supervision period of the transmitter.

No Point Text If Area Text

This checkbox affects the location text shown on the Alarm Screen. If this checkbox is checked and the alarm is determined to be within a predefined area, only the area text is displayed (any receiver location text is suppressed). Typically, this checkbox should be checked.

Output includes Subscriber ID

If this checkbox is checked, any time the system prints or displays text for an alarm or test the subscriber's ID number is displayed. Otherwise, the subscriber's ID is not shown.

Output includes Transmitter ID

If this checkbox is checked, any time the system prints or displays text for an alarm or test the transmitter ID number is displayed. Otherwise, the transmitter ID is not shown. Typically, this checkbox would not be checked.

Limit Alarms to 1 Transponder

This box should not be checked. It is used only in a system where all transponders operate on areas separate from each other. It prevents all interactions between receivers on different transponders. Typically this is undesirable and there is now a selection on an individual transponder basis to accomplish this feature.

Option 2

This checkbox is for a future option and at this time it has no function. Leave this checkbox unchecked.

Require Alarm Report

If this checkbox is checked, the operator is prompted to complete an Alarm Report when the alarm is reset from the screen. If the responding officer is required to complete the report or if no system report is desired, this box should not be checked. If the operator should complete the report, check this box.

Security Alarms Silent

If this checkbox is checked, alarms transmitted by Security or Watchman Transmitters are to be silent. This alerts the operator at the central console, but does not sound the sirens of the alert units or the horns in the receivers.

Installer Alarms Silent

If this checkbox is checked, alarms transmitted by transmitters issued to installation company representatives and visitors are to be silent. The operator at the central console is alerted, but the sirens of the alert units or the horns in the receivers are not sounded. Typically, this checkbox is checked.

Alarm Voice Output

If this checkbox is checked, predefined sound (.WAV) files can be played at the alarm console for specific alarm types. Typically, this checkbox is not checked.

Show Personal Data

If this checkbox is checked, personal height, build, hair, and eye color data displays on the alarm screen.

No Receiver Icons

If this checkbox is checked, individual receiver icons are not shown on the alarm map display. Typically, this checkbox is checked.

Show Tests On The Map

If this checkbox is checked, tests from Subscriber's Transmitter appear on the normal map screen as OK or FAIL icons. This signifies a successful test by a valid subscriber or an attempted test transmission from a transmitter not in the Subscriber Database. This option does not affect the display the subscriber receives from a receiver or alert unit's strobe. Typically, this checkbox is checked.

All Pager Confm Not Req'd

If checked, the confirmation pager message is not sent to any of the pager if the alarm is acknowledged by an acknowledgement transmitter.

Option 4

This checkbox is for a future option and at this time has no function. Leave this checkbox unchecked.

Option 5

This checkbox is for a future option and at this time has no function. Leave this checkbox unchecked.

Auto Silence Alarm In X Seconds

This box determines the length of time that the sirens and horns sound before being automatically silenced by the central console. When the sounders are automatically silenced in this way, the central console remains in its Alarm Mode. The numerical value is in seconds and it can be set between 0 and 9999. Typically, this value is set to prevent violating local noise ordinances. It defaults to 240 seconds (4 minutes.).

Recall Operator In X Seconds

This box determines the length of time before a recall alert is issued to the operator at the central console when an alarm displays. If neither the mouse nor any key was actuated for the specified length of time, the central console resounds the alarm sound once. This feature prevents inadvertently ignoring an active alarm event. The numerical value is in seconds that can be set between 0 and 240. Typically this would be set to 60 seconds.

On Outside Tests Flash Strobe For X Seconds

The entry in this box controls the approximate length of time the strobe on an alert unit flashes to signify a successful transmitter test. The value is in seconds, and can be set between 0 and 15. Typically, it is set to 5 seconds.

Man Down Delay Timer X Seconds

This value controls the time that a transmitter must be in a man down condition before a man down alarm displays. Typically, it is set to 10 seconds. Setting this value too short causes inadvertent man down alarms to be generated.

Man down jitter timer 'X' Seconds

This value controls the time that a transmitter will not be considering any man down alarm if man down alarm is received immediately after restore and before jitter time expire. This setting will not be used in normal system.

Auto Reset Comm Ports 'X' Hours

This value controls the time that all the comm ports in the system will be automatically reset after configured duration. This setting is used only if any communication failure is observed and should not be used unnecessarily.

End Of Shift Reminder

A check in this box causes a prompt to appear on the central console each 5 min. for 30 min. prior to the end of each shift if there are Incident Reports that were not yet completed. Responding officers should complete Alarm Reports before the end of their shift.

First, Second, Third Shift Reminder

The entries in these fields are the times (24-hr. clock) at which the central console prompts the operator that one or more Incident Reports have not been completed. Prompts are given only if the **End of Shift Reminder** field is selected.

Database Find Level

This is the minimum receive level (1 to 255) that must be heard before the system automatically enters the transmitter in the Subscriber Locate Screen. It determines the distance the subscriber's transmitter must be within the specified ID capture receiver (set in the System Preferences Screen) before the system recognizes the test.

Locate Test Level

This is the minimum receive level (1 to 255) that must be heard before the system accepts a test generated by a transmitter other than a guard, to be printed with a location. It determines the distance the transmitter must be from a receiver before the system recognizes the test and prints the location. If the transmitter is too far away from the receiver, that receiver's green light does not display, and the guard knows to move closer to the receiver for the test to register.

Guard Tour Level

This is the minimum receive level (1 to 255) that must be heard before the system accepts a test generated by the guard's transmitter to be entered as a location in the Guard Tour Report. It determines the distance the guard's transmitter must be from a receiver before the system recognizes the test and creates the guard tour entry. If the guard is too far away from the receiver, that receiver's green light does not display and the guard knows to move closer to the receiver for the test to register.

Guard Tour Minutes

This setting controls the time spacing, in minutes, for entries of the guard's current location in the automatically generated Guard Tour Report. If set to 15 min., an entry is generated each 15 min. the guard's transmitter is within range of the system.

Pop-up Trouble Box Contact Information"

Each yellow Pop-up Trouble Box appears on the central console advises the operator of system problems and contains specific instructions. Entries in this text box are displayed in the System Trouble Reported Screen whenever a system problem occurs that requires attention. This information usually includes the name and telephone number of the designated Security Escort maintenance technicians.

3.2.4 System Defaults Screen

This screen allows the names for each class of subscribers to be changed to match the Security Escort System.

Titles entered into the **Subscriber Name** field in the Subscriber Database are entered here. The system alphabetizes the Subscriber Database entries by last name. When a title is entered after the last name, the entry is alphabetized incorrectly by title. Entering the titles used prevents this problem.

The labels for the four **Information label** fields, in the Subscriber Database, are also changeable here.

Figure 27: System Defaults Screen

3.2.5 System Labels Screen

The alarm type definitions are modified to the customer's requirements in Figure 28.

Figure 28: System Labels Screen

3.2.6 Print System Reports Screen

This screen allows System Reports to be printed now, scheduled for printing each night at midnight, or weekly on Sunday at midnight. To print a report or reports, check the left-hand box for each report desired and click **Print**. Check **Midnight report** or **Sunday only** checkbox to automatically schedule that report at those times.

Figure 29: Print System Reports Screen

Daily Test Report

Report of testing by classes of subscriber for the last 24 hrs. broken down by hour.

Low Battery Report

Report of all subscriber transmitters currently reporting low battery.

Not Testing Report

Report of all subscriber transmitters that have not tested their transmitters within the last 28 days.

Receivers Not Heard From Report

Report of all receivers that have not heard transmissions recently. This could indicate a problem with that receiver's ability to hear alarm and test transmissions.

Daily Trouble Report

Report of all the troubles currently being reported by transponders, receivers, and alert units.

Guard Tour Report

This selection does not generate a printed report. However, the **Midnight report** and **Sunday only** checkboxes must be checked to write a file of the guard tour information. Another application like Microsoft Excel can sort and print the desired reports.

Guard Tour Exception Report

The Guard Tour Exception Reports collected within the last day. Not currently implemented.

New Alarm Reports

Alarm reports for all of the new alarms received by the system.

Fail To Test Letters

Notices to all of the subscribers that have not tested within the last 28 days. Not currently implemented.

Weekly Subscriber Test Report

Report of subscriber testing for the last seven days broken down by hour.

Weekly Security Test Report

Report of security personnel testing for the last seven days broken down by hour.

Weekly Watchman Test Report

Report of watchman personnel testing for the last seven days broken down by hour.

Weekly Maintenance Test Report

Report of maintenance testing for the last seven days broken down by hour.

Subscriber Check-in Report

Report of all subscribers that failed to check-in during the last scheduled check-in period.

Supervision Location Report

Report of all supervision enabled subscribers and their last known location.

Print

Clicking this button prints all reports that are checked in the left-hand check boxes.

Print Report Now

Reports with these check boxes checked are printed when the **Print** button is checked.

Midnight Report

Reports are automatically generated each midnight for all reports that are checked in the **Midnight Report** check boxes.

Sunday Report

Reports are automatically generated each Sunday at midnight for all reports that are checked in the **Sunday Report** check boxes.

3.2.7 Alarm Report Generation Screen

This dialog allows the alarm reports to be generated in CSV format.

Figure 300: Alarm Report Generation Screen

To print an alarm report, you may directly enter the date or press the ellipsis (...) button in **from date, to date** box and select **from time, to time** from the respective dropdowns. An alarm report can also be printed based on the subscriber details. Select the Subscriber ID, Subscriber Name, Transmitter ID or Subscriber Type from the dropdowns to generate an alarm report.

The alarm report can be sorted by Alarm Time, Transmitter ID, Subscriber Name, Problem Type, Subscriber Type, by using the **Sort By** dropdown. You can change the report name and file location by pressing the ... button. Clicking the **Export** button saves the generated report to specified file. Clicking the **Cancel** button cancels the report generation and exits from the Alarm Report Generation dialog.

3.2.8 Schedules Screen

This selection informs management of the ten-time of day/day of week schedules and holidays. The top portion of the display shows the ten-time-of-day/day-of-week schedules that Security Escort supports. For each schedule, there is an indication the schedule is currently active or armed (ACT); otherwise, the schedule is disarmed (OFF).

This schedule defines the check-in times

One of the ten schedules can be used to define the check-in times for those subscribers that must check-in. Click on the schedule for the check-in schedule, highlighting it. Then check this checkbox, to set the selected schedule as the check-in schedule. Both the arm time and disarm time must be programmed for every day the check-ins must take place. The arm time is the start of the check-in schedule and it must occur before the disarm time that marks the end of the check-in schedule for that day.

Edit Schedule Times

Clicking this button displays the Edit Schedule Times Screen so the day of week arm and disarm schedule times can be edited.

View Alarm Groups

Clicking this button displays the View Alarm Groups Screen. This screen shows the alarm groups assigned to the selected schedule and their current arming state.

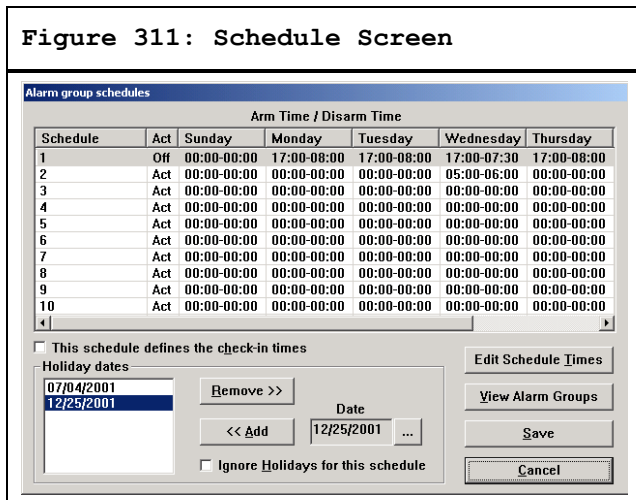
Ignore Holidays for this Schedule

Each schedule can use the holiday dates as exceptions. If the **Ignore Holidays** checkbox is checked or the indicated holiday dates, the schedules are activated (armed) that entire day. If the **Ignore Holidays** checkbox is not checked, the normal action of the schedules take place on the holiday dates.

You may directly enter the date or press the ... button. The holiday dates do not accept wildcards so you must enter an entire date.

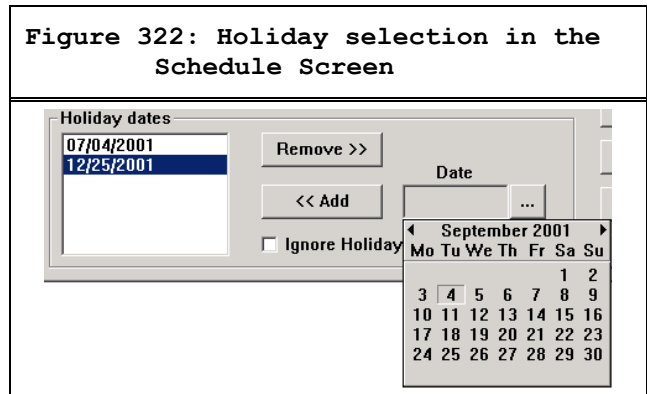
Figure 32 shows a list of holidays that can be used as exceptions to the one or more of the ten schedules.

Figure 311: Schedule Screen



For each day-of-the-week, the arm time (time the schedule becomes active) and disarm time (time the schedule becomes inactive) are displayed. To edit the arm and disarm times, click **Edit Schedule Times**. Double clicking the number of the schedule allows you to name the schedules.

Figure 322: Holiday selection in the Schedule Screen



Ellipsis (...)

Clicking this button displays a calendar where you can graphically select a date.

Remove >>

Clicking this button removes the selected date from the holiday dates list.

<< Add

Clicking this button adds the date shown to the holiday dates list.

3.2.9 Edit Schedule Times Screen

This screen allows the arming and disarming times to be programmed for each of the days of the week. All times are expressed in 24-hr. time (00:00 to 23:59). Each schedule has one arm time and one disarm time for each of the seven days of the week.

If both the arm time and disarm time are programmed to 00:00, the schedule is active (armed) for the entire day.

If the arm time is 00:00 and the disarm time is programmed, from midnight to the programmed disarm time, the schedule is active (armed) and from the disarm time to the end of the day the schedule is off (disarmed).

If the disarm time is 00:00 and the arm time is programmed, from midnight to the programmed arm time the schedule is off (disarmed) and from the arm time to the end of the day the schedule is active (armed).

If both the disarm time and the arm time are programmed and the disarm time occurs before the arm time (normal - eight-to-five day), from midnight to the programmed disarm time the schedule is active (armed). From the disarm time to the arm time, the schedule is off (disarmed). From the arm time to the end of the day, the schedule is active (armed).

If both the disarm time and the arm time are programmed and the arm time occurs before the disarm time, from midnight to the programmed arm time the schedule is off (disarmed). From the arm time to the disarm time, the schedule is active (armed). From the disarm time to the end of the day, the schedule is off (disarmed).

Arm Time

This is the time the schedule becomes active (on or armed) for the selected day of the week. Times are expressed in 24-hr. time (00:00 to 23:59).

Disarm Time

This is the time the schedule goes off (disarmed) for the selected day of the week. Times are expressed in 24-hr. time (00:00 to 23:59).

Day of the Week

Select the day you want to change the time. The arm time and disarm time are programmed separately for each day of the week. You must individually select each day of the week and set the desired times.

3.2.10 View Alarm Groups Screen

Figure 34 shows the alarm groups assigned to the selected schedule and their current arming state. The on and off states indicate the alarm group is under manual control. Auto is under control of the selected schedule. The alarm group is armed if the schedule is active.

Figure 333: Edit Schedule Time Screen

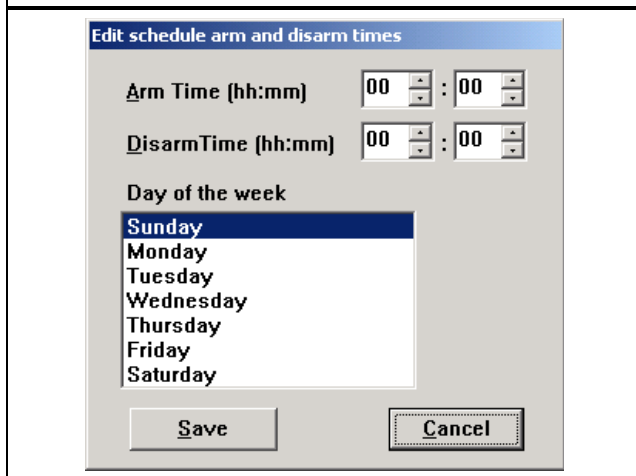
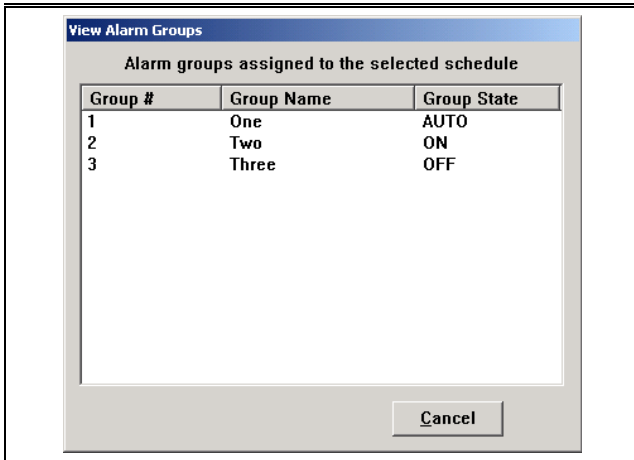


Figure 344: View Alarm Groups Screen

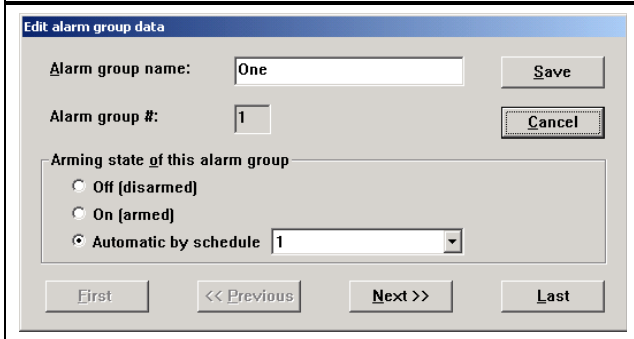


3.2.1 Alarm Groups Screen

This selection allows setup and arm/disarm control of the 99 alarm groups. Any number of point transmitters can be assigned to an alarm group in the Subscriber Database's Advanced Screen. Each transmitter can only be assigned to one alarm group.

An alarm group can be manually armed and disarmed or assigned to a schedule to automatically arm and disarm the alarm group.

Figure 355: Alarm Groups Screen



Alarm Group Name

Enter a descriptive name to identify the function of the points in this alarm group.

Alarm Group #

This is the number of the alarm group (1 to 99).

Arming State of this Alarm Group

The **Off**, **On**, and **Automatic by schedule** fields control the arming state of this alarm group.

Off (disarmed)

Clicking this button disarms the alarm group. The alarm group remains off (disarmed) until it is manually changed in this screen to **On** or **Automatic by schedule**.

On (armed)

Clicking this button arms the alarm group. The alarm group remains on (armed) until it is manually changed in this screen to **Off** or **Automatic by Schedule**.

Automatic by Schedule

Clicking this button assigns the alarm group's arming state to be controlled by the indicated schedule. When the schedule is active (on or armed), the alarm group is armed. When the schedule is off (disarmed), the alarm group is disarmed. Any number of alarm groups can be assigned to the same schedule.

First

Clicking this button takes you to alarm group 1.

Previous

Clicking this button takes you to the next lower alarm group from the one displayed. It does not wrap around. It is disabled at alarm group 1.

Next

Clicking this button takes you to the next higher alarm group from the one displayed. It does not wrap around. It is disabled at alarm group 99.

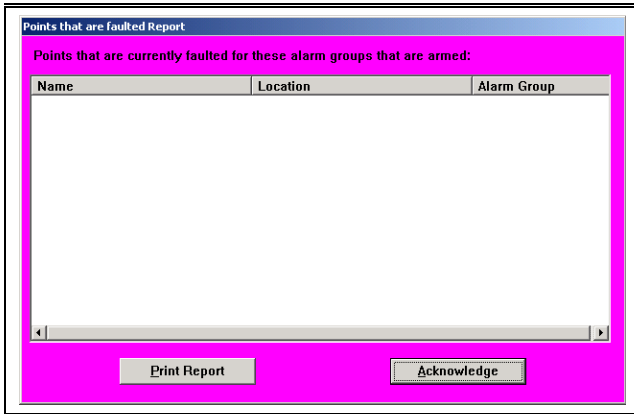
Last

Clicking this button takes you to alarm group 99.

3.2.72 Alarm Group State Screen

This selection displays a list of the alarm groups that are armed and have one or more transmitters (points) faulted. The points are presented because they were not restored when their automatic schedule armed or there was an alarm while the alarm group was on.

Figure 366: Alarm Group State Screen



Print Report

Clicking this button prints the displayed data to the report printer.

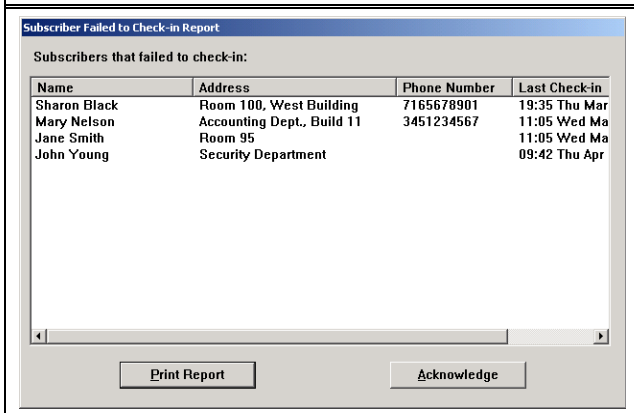
Acknowledge

Clicking this button closes the screen if it was selected from the menu. If the screen appears automatically at the arm time of an alarm group's automatic schedule because they were not restored when their automatic schedule armed or there was an alarm while the alarm group was on, you must enter your password to the acknowledge the screen and remove it from this computer's (and all other computer workstations) screens.

3.2.83 Current Check-in Status Screen

This selection displays a list of the subscribers that are required to check-in and failed to do so during the last check-in period. Also shown are their addresses, phone numbers, and the last time they checked in.

Figure 377: Current Check-in Status Screen



Print Report

Clicking this button prints the displayed data to the report printer.

Acknowledge

Clicking this button closes the screen if it was selected from the menu.

If the screen appeared automatically at the end of the check-in period because some subscribers failed to check-in, you must enter your password to acknowledge the screen and remove it from this computer's (and all other computer workstations) screens.

3.2.94 Clear Screen

When selected, clears the map of any icons and returns to the default map display.

3.2.105 Output Verification

When selected, the system is scanned to verify that all alarm outputs are in the correct state. Any output found in the wrong state is corrected.

3.2.116 Synchronize System Time

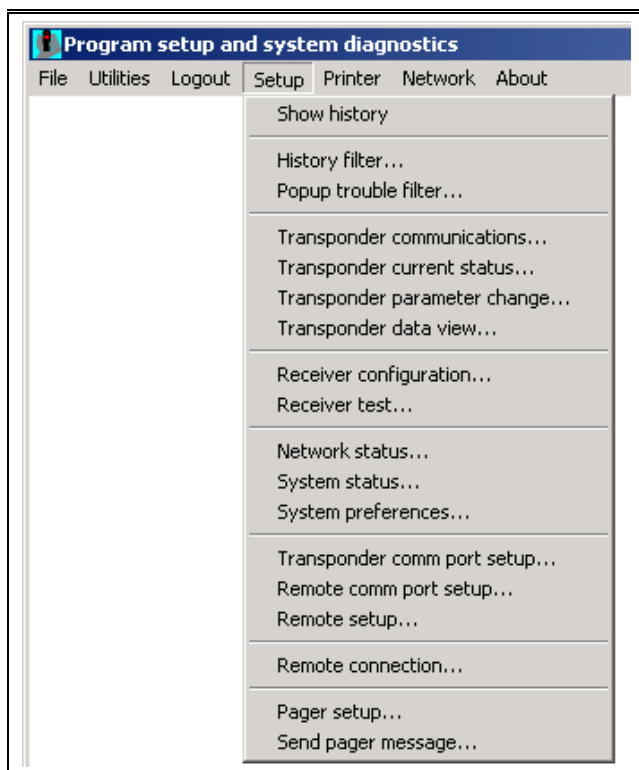
Selecting this option on the master computer causes the time on the slave and all of the workstation computers to be updated to the master computer's time.

3.3 Setup Menu

3.3.1 Show History

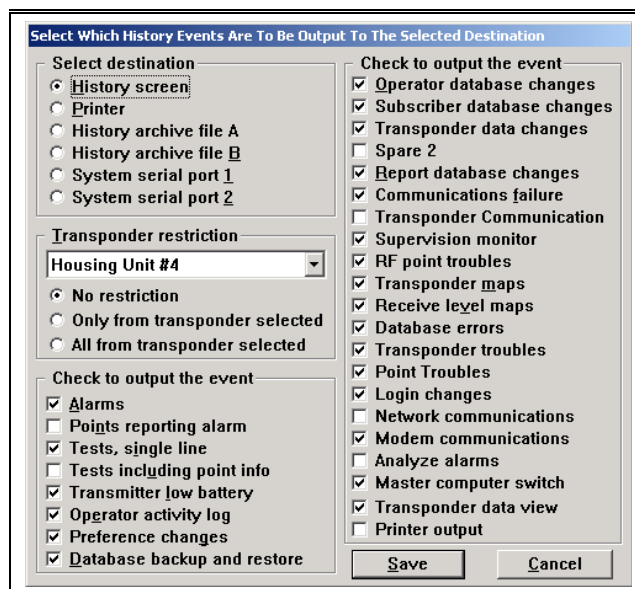
When selected, the default map display is replaced by a scrolling text display showing the most recent events that occurred in the system. The events displayed can be selected in the History Filter Screen under the Setup Menu. After **Show History** is selected, this selection changes to **Show Map**.

Figure 388: Setup Menu



3.3.2 History Filter Screen

This screen selects the classes of events recorded (sent to) for specific output devices. The **Select Destination** box selects the History Screen, printer, history files, and system serial ports. Notice when this selection is changed, the checked items also change. There is a different set of events output for each destination selected. For each destination, the events to be output must be individually configured.



History Screen

This option selects the events displayed on the computer screen when **Show History** is selected.

Printer

This option selects the events sent to the printer.

History Archive File A

This option selects the events sent to the a_audit.txt file stored in the Security Escort sub-directory (typically C:\escort\a_audit.txt). There is a minimum set of events that cannot be disabled, so they are always recorded.

History Archive File B

This option selects the events sent to the b_audit.txt file stored in the Security Escort sub-directory (typically C:\escort\b_audit.txt).

System Serial Port 1

This option selects the events sent to the System Serial Port 1. System Serial Port 1 is assigned a physical comm port in the Remote Comm Port Setup Screen and the **History Filter Output** field must be set in the Remote Setup Screen.

System Serial Port 2

This option selects the events sent to the System Serial Port 2. System Serial Port 2 is assigned a physical comm port in the Remote Comm Port Setup Screen and the **History Filter Output** field must be set in the Remote Setup Screen.

Transponder Restriction

This option selects a transponder for the following restrictions:

Figure 399: History Filter Screen

- **No Restriction:** This selection typically is left at this setting at all times. The output is not restricted by an individual transponder.
- **Only From Transponder Selected:** The selected events are only output if they were reported from the transponder selected in the Transponder Restriction above.
- **All from Transponder Selected:** All events are reported from the transponder selected in the Transponder Restriction above. The selected events are reported from all other transponders in the system.

Alarms

Outputs the information about an alarm including location, but not the transponder and receiver levels. This is the data typically sent to a printer.

Points, Reporting Alarm

Outputs the transponder and receiver levels for an alarm. Typically, this is the data too detailed to send to a printer and is used for diagnostics, not normal system operation.

Tests, Single Line

Outputs the simple information about a test. Typically, this is the data normally sent to a printer.

Tests Including Point Info

Outputs the transponder and receiver levels for a test. This is the data usually too detailed to send to a printer and is used for diagnostics, not normal system operation. If this option is selected, Test, Single Line above, would not be selected for the same output device.

Transmitter Low Battery

Outputs low battery reports received from transmitters.

Operator Activity Log

Outputs all other operator activity (audit trail) not covered by specific event selections.

Preferences Changes

Outputs all changes made to system preference selections.

Database Backup and Restore

Records all database backup and restore activity.

Operator Database Changes

Records all changes to the operator database.

Subscriber Database Changes

Records all changes to the subscriber database.

Transponder Database Changes

Records all changes to the transponder database.

Spare 2

Not currently implemented. Leave unchecked.

Report Database Changes

Records all changes to the Alarm Report Database.

Communications Failure

Records all communication failures and restorals.

Transponder Communication

Records all communications to transponders. This selection is only used for engineering diagnostics. Leaving this item selected generates a significant amount of history and fills up the hard disk drive quickly. Leave this item unchecked.

Supervision Monitor

Reports changes in the supervision status for all transmitters that are being supervised.

RF Point Troubles

Outputs all troubles reported by RF points. Check this item to monitor problems with RF points.

Transponder Maps

Outputs all transponder status maps. This selection is only used for diagnostics. Leave this item unchecked.

Receive Level Maps

Outputs all maintenance alarm receive level maps. This selection is only used for diagnostics. Leave this item unchecked.

Database Errors

Outputs all reported database errors. This item is checked.

Transponder Troubles

Outputs all reported transponder troubles. This item is checked for devices used to monitor problems.

Point Troubles

Outputs all reported receiver and alert unit troubles. This item is checked for devices used to monitor problems.

Login Changes

Reports all new system operator login and logout activity.

Network Communications

Records all communications between networked computers. This selection is only used for engineering diagnostics. Leaving this item selected generates a significant amount of history and fills up the hard disk drive very quickly and may bog down the system during high traffic times. Always leave this item unchecked.

Modem Communications

Records all communications to the modem for remote communications and pager access. This selection is only used for diagnosing pager communication problems. Leave this item unchecked.

Analyze Alarms

This option outputs data allowing an engineer to evaluate how well the location algorithm is performing. Leave this item unchecked.

Master Computer Switch

Records when the master and slave computers switch roles.

Transponder Data View

Allows the data created by the Transponder Data View Screen to be output. This selection is only used for engineering diagnostics. Leave this item unchecked.

Printer Output

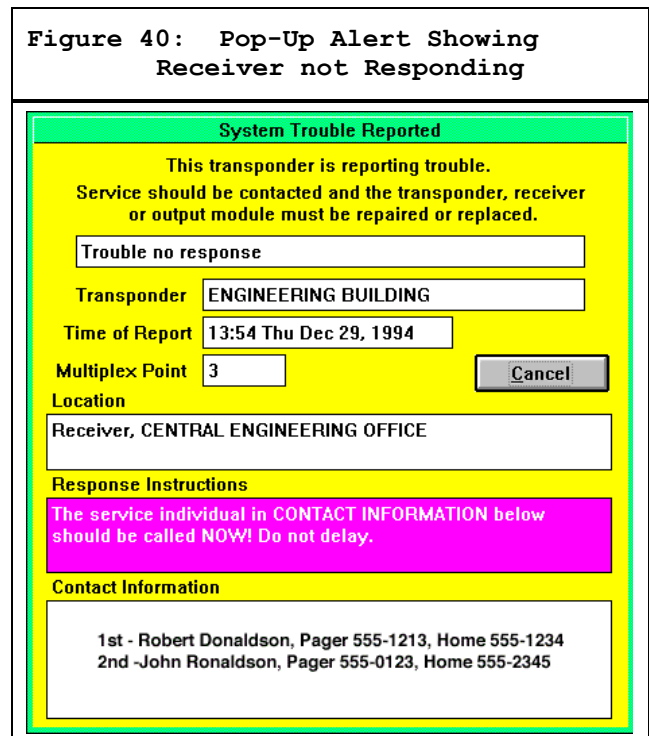
Allows the data being sent to the printer to be sent to other outputs. This item is unchecked.

3.3.3 Pop-up Trouble Filter

The Security Escort System contains many built-in self testing features. Each transponder tests the condition of the receivers and alert units connected to it.

When the transponder finds a device reporting a trouble condition, it communicates the problem and the device identity to the central console. This generates a brief alert tone, displays a pop-up message for the operator, and sends an optional pager message. The message indicates the nature of the trouble and instructs the operator on the proper course of action. The status of the device is recorded in the Transponder Current Status (See Section 3.3.10 *Transponder Current Status* Screen) file under the **Setup** Menu. The event is recorded on the hard disks of both the main and backup computers and on the printout.

Figure 40: Pop-Up Alert Showing Receiver not Responding



Selects which trouble categories cause pop-up messages to appear on the central console or be sent to the service pager. The troubles described below are always recorded in the Transponder Current Status Screen, but might or might not produce a pop-up display or pager message, depending on the selections made.

Figure 411: Pop-up Trouble Filter Screen

3.3.4 Transponder Troubles

Popup

All troubles with these checkboxes checked present a popup screen to the operator when the respective trouble becomes active.

Pager

All troubles with these checkboxes checked send a page to the service pager when the respective trouble becomes active.

Communications Failure

To continually assure that communications between the central console and each transponder are functioning properly, each transponder is required to send a message to the central console periodically. If there is no response from the transponder, the central console displays a Communications Failure warning on the central console and records the condition in the audit file.

If a transponder determines it lost communications with the central console, it assumes control of the outputs of the devices connected to it and transmits I'M OK messages until it is acknowledged by the central console.

transmission is received by one or more of the receivers attached to the transponder, the transponder activates any alert units attached to it as well as the horns and red LED's on any of its receivers which detected the alarm transmission. Since the transponder does not have access to the Subscriber Database, it must assume that all transmitters are valid, so even unauthorized (not in the Subscriber Database) transmitters produce audible alarm indications (if the System is set for audible alarms in the Set Security Preferences Screen).

The central console also attempts to reestablish communications by continually requesting transmissions from the transponder and listening on the communications channel. When communications are restored with the central console, the transponder transmits any alarm and trouble conditions that occurred during the communications loss, and control of the horns, LED's, strobes, and sirens reverts to the central console.


This approach to managing a communications loss assures that alarm events can not go undetected even if the central console is out of operation temporarily.

AC Loss

The transponder senses when it loses AC power and reports the condition to the central console. After a few seconds delay, the central console, displays a pop-up alert and records the condition in the audit file. See *Section 3.3.10 Transponder Current Status Screen*.

Low Battery

Periodically during normal operation, the transponder tests its battery. If the test fails, it immediately reports the condition to the central console. After a few seconds delay, the central console displays a pop-up alert and the condition is recorded in the audit file.

 If during this loss of communications, an alarm

Tamper

The transponder immediately senses and reports the actuation of its tamper switch. The central console immediately displays a pop-up alert and records the condition in the audit file. Tamper Reports are not delayed by the pop-up trouble and pager delay.

Remote Key Activation

The transponder immediately senses and reports the activation (shorting) of its remote key input when it is enabled in the Transponder Parameter Screen. The central console displays a pop-up alert and records the condition in the audit file.

Remote Key Tamper

The transponder immediately senses and reports the fault (open) of its remote key input when it is enabled in the Transponder Parameter Screen. The central console immediately displays a pop-up alert and records the condition in the audit file.

Transponder Startup

The transponder reports to the central console when it first starts up. This can be caused by a technician turning the transponder on or by a watchdog failure of the on board microprocessor. The central console immediately displays a pop-up alert and records the condition in the audit file.

Bus Faults

When the transponder is unable to communicate to any receivers or alert units on one or more of its multiplex busses, it immediately reports the condition to the central console. The central console reports the condition by means of a pop-up alert if the condition persists more than a few seconds. The condition is also recorded in the audit file.

3.3.5 Mux Bus Point Troubles**AC Loss**

The microprocessor of the alert unit detected the absence of AC power. Loss of AC power affects only the strobe and siren functions of the alert unit. Batteries provide backup power for the strobes and sirens. The logic and communications functions derive their power from the multiplex bus.

Low Battery

The alert unit tested for a low battery condition and the test failed.

Tamper

Whenever the cover is removed from a receiver or alert unit, the on-board microprocessor detects the tamper and it is reported to the transponder. Tamper reports are not delayed by the pop-up trouble and pager delay.

No Response

Whenever a receiver fails to respond to a command from the transponder, a No Response message is sent by the transponder to the central console. This can occur if a multiplex bus wire is cut or a device is damaged.

Jamming

Each receiver monitors the level of radio energy being received at all times. If the level exceeds a preset threshold, for a preset length of time, the on-board microprocessor reports jamming.

Output Device Error

The transponder generates this message when it commands a receiver or alert unit to activate or deactivate an output device (siren, strobe, horn, or LED) and the device fails to respond correctly.

Bad Checksum

This message is generated by the transponder and sent to the central console whenever the transponder detects message errors in the communications between receivers and alert units.

3.3.6 Transmitter Supervision Monitor**Known Transmitters**

To continually monitor the status of all transmitters programmed in the database that send periodic supervision transmissions. If any monitored transmitters stop sending supervision transmissions, a pop-up trouble is displayed.

Unknown Transmitters

To monitor for periodic supervision transmissions from transmitters not programmed in the database a pop-up trouble displays if transmissions from transmitters not programmed in the database are received.

Monitored Periods

This is the number of supervision intervals that are consecutively missed before a pop-up screen reports a specific transmitter stopped reporting supervision transmissions.

3.3.7 Communications Port Monitor

Comm Port Overload

A pop-up trouble screen displays if the communications traffic to the transponders exceeds the system is capability.

Network Comm Failure

A pop-up trouble screen displays if the communications between the master and slave computers fails.

3.3.8 Delay To Ignore Troubles That Auto Reset

Network Comm Failure

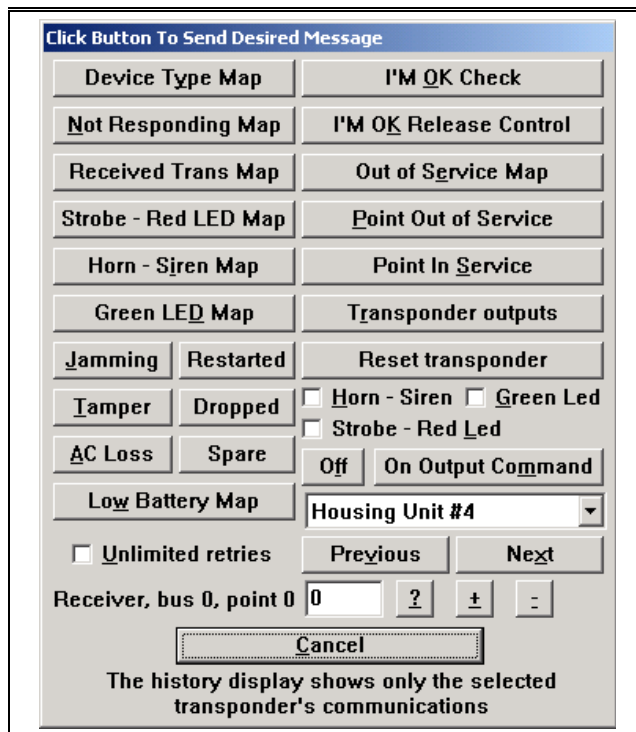
A pop-up trouble screen displays if the communications between the master and slave computers fails.

Pop-up Trouble and Pager Delay

The delay in seconds before a trouble displays on the computer screen. If a restoral for a trouble is received before a trouble is displayed (this delay expires), the trouble and the restoral's ignored. Tamper troubles are not delayed.

3.3.9 Transponder Communications Screen

From the central console, it is possible to perform detailed diagnostic tests using the Transponder Communications Screen. From this screen, the operator can request maps indicating the status of each device connected to a given transponder, and can control individual devices, turning LED's, horns, strobes, and sirens on and off. The Transponder Communications Screen appears on the right when it is opened, allowing the History Screen to be viewed while the screen is open. This makes it possible to view the results of map commands issued from the console.



Map Commands

Diagnostic map commands are used to determine the status of all devices (connected to the selected transponder) with a single command. Maps are displayed on the History Screen as an array of rows and columns, corresponding to point addresses and bus numbers. The status of a particular device is shown by a "1" or "0" (zero) with "1" signifying the true state. The map location, corresponding to a device that is not responding to the transponder, contains a "1" when a Not Responding Map is selected.

Similarly, a "1" is displayed in response to a Tamper Map in locations that correspond to devices in a tampered state. All other locations display a "0" (zero), "a" - (if there is no device assigned to the location), or a "x", there is a device connected to the system at that address, but it is not in the Transponder Database.

Figure 422: Transponder Communications Screen

Device Type Map

Unlike all other types of map, the device type map has two characters in each possible device location. The right most character indicates the device type. A "5" indicates a receiver, "3" indicates an alert unit, and "7" indicates that the Transponder Database shows a device in that location but it is not currently communicating with the transponder. The left character indicates the following: "0" (zero), the device is in its normal state, "1", the device is off normal, and "x" there is a device connected to the system at that address, but it is not in the Transponder Database. (Usually this results from an error during data entry in the Transponder Database.)

Not Responding Map

Requests a map of all the points that are not responding (missing) to the system on this transponder. The **Received Transmission Map** button produces a map display with one in the locations corresponding to receivers that are missing from the system. A "0" (zero) indicates that the point is responding. An "x" indicates there is a device connected to the system at that address, but it is not in the Transponder Database.

Received Transmission Map

As a means of self-diagnosis, the system software periodically reviews the receivers, that have not received an alarm or test transmission. This list is printed as a part of the daily System Status Report and is a tool for assessing the health of the system. The **Received Transmission Map** button produces a map display with "1" in the locations corresponding to receivers which received transmissions. Each time this map is read, the Received Transmission Map image is cleared in the transponder.

Strobe - Red LED Map

Requests a map of all the points on this transponder that have their Strobe - Red LED on. The **Strobe - Red LED Map** button displays a map with "1" in the locations corresponding to points which have their outputs on. A "0" (zero) indicates that the output is off.

Horn - Siren Map

Requests a map of all the points that have their horn or sirens on, on this transponder. The **Horn - Sirens Map** button displays a map with "1" in the locations corresponding to points which have their outputs on. A "0" (zero) indicates that the output is off.

Green LED Map

Requests a map of all the points on this transponder that have their Spare outputs - Green LED on. The **Green LED Map** button displays a map with "1" in the locations corresponding to points which have their outputs on. A "0" (zero) indicates that the output is off.

Jamming

Requests a map of all the receivers that are currently reporting RF jamming to the system. The **Jamming** button displays a map with "1" in the locations corresponding to receivers that are reporting jamming. A "0" (zero) indicates that the receiver is not jammed.

Tamper

Requests a map of all the points that are currently reporting a tamper condition to the system. The **Tamper** button displays a map with "1" in the locations corresponding to points that are reporting tamper. A "0" (zero) indicates points that are not tampered.

AC Loss

Requests a map of all the alert units that are currently reporting an AC power failure to the system. The **AC Loss** button displays a map with "1" in the locations corresponding to alert units that are reporting AC Loss.

Restarted

Requests a map of all the points that are powered up or had a watchdog failure to the system. The **Restarted** button displays a map with "1" in the locations corresponding to points that are restarted.

Dropped

Requests a map of all the receivers that have dropped one or more receptions due to high traffic. The **Dropped** button displays a map with "1" in the locations corresponding to receivers that dropped one or more transmissions.

Spare

This is a future option. Not implemented at this time.

Low Battery Map

Requests a map of all the alert units that are currently reporting a Low Battery to the system. The **Low Battery Map** button displays a map with "1" in the locations corresponding to points that are reporting Low Battery.

I'm OK Check, I'm OK Release Control Buttons

These buttons are used to diagnose and correct communications problems between the central console and the transponder. The system software requires that each transponder send a message to the central console periodically if no other communications have taken place. These messages are called I'm OK messages. If for some reason the communications link between the central console and the transponder fails, the transponder recognizes the fact when its I'm OK transmissions are not acknowledged by the central console. When the transponder has retried transmitting an I'm OK message or any other message six times without acknowledgment, it assumes control of the outputs (LED's, horns, strobes, and sirens) on devices connected to it and modifies the message to indicate that it is still OK and has taken control. These messages are transmitted once per minute until communications are reestablished.

The **I'm OK Check** button requests that the transponder send an I'm OK message. This is used to determine if a transponder has taken control of its outputs. The **I'm OK Release Control** button generates a command to the transponder to release control back to the central console. Normally, the central console automatically generates a Release Control message upon the re-establishment of communications following a failure.

Out Of Service Map

The Out Of Service Map shows those points (receivers or alert units) that are currently out of service. Points may be taken out of service and returned to service by selecting the point using MUX Bus Point Screen in the bottom right corner of the screen and clicking the **Point Out Of Service** or **Point In Service** button. Points can be selected by typing in the point number or by using the [+] and [-] buttons, or the [?] button.

Point Out Of Service

Clicking this button takes the currently selected point out-of-service. That point no longer responds to the system, as if it was disconnected. Use this function with caution.

Point In Service

Clicking this button restores the currently selected point to an in-service condition. That point returns to normal function.

Transponder Outputs

Requests the current state of the siren and strobe outputs on the transponder.

Reset Transponder

Clicking this button resets the transponder as if it was just powered up. Any test or alarm processing that was in progress at the time is lost.

Horn - Siren

If this checkbox is checked, the horn output of a receiver or the siren output of an alert unit is turned on if **On Output Command** is clicked, or off if **Off** is clicked. If this checkbox is not checked, the state of this output is not changed.

Green LED

If this checkbox is checked, the green LED output of a receiver or the spare output of an alert unit is turned on if **On Output Command** is clicked, or off if **Off** is clicked. If this checkbox is not checked, the state of this output is not change.

Strobe - Red LED

If this checkbox is checked, the red LED output of a receiver or the strobe output of an alert unit is turned on if **On Output Command** is clicked, or off if **Off** is clicked. If this checkbox is not checked, the state of this output is not changed.

Off

When clicked, the checked horn-siren, green LED and strobe-red LED outputs are turned off for the selected point on the selected transponder. If the output does not change, click **On Output Command** and click **Off** again.

On Output Command

When clicked, the checked horn-siren, green LED, and strobe-red LED outputs are turned on for the selected point on the selected transponder. If the output does not change, click **Off** and then click **On Output Command** again.

Transponder

Selects the transponder you desire to communicate with.

Previous

Returns to the previous transponder.

Next

Advances to the next transponder.

Bus X Point Y

This field displays the current bus number and point number. The actual point number may be entered in the field to the right.

?

Opens up the Select Point Screen.

+

Advances to the next point.

-

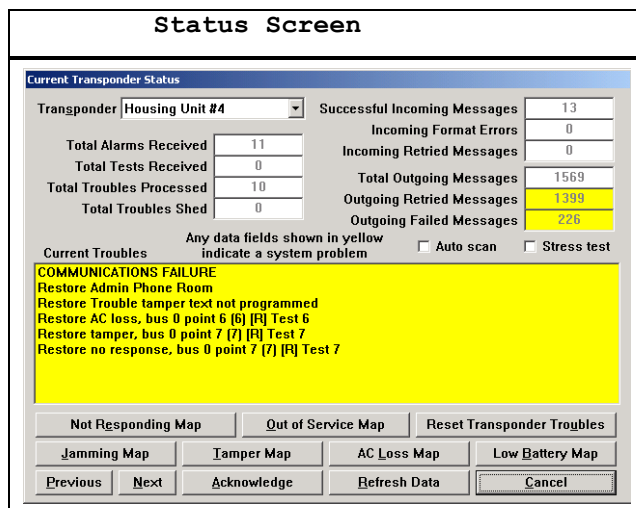
Returns to the previous point.

Unlimited Retries

When this box is checked, the central console continues trying to send commands to a transponder even if the commands are not being acknowledged. (Normally, the central console would cease after six retries and declare a communication failure.) When this screen is closed, the system reverts to the normal six retries.

3.3.10 Transponder Current Status Screen

This screen, accessible from the **Main Menu** under the **Setup** selection, provides a history of communications involving the transponder selected in the transponder box. It also provides several buttons, that can be used to diagnose problems with the transponder and any of its receivers or alert units.



Transponder

Selects the transponder you want to see the status of.

Total Alarms Received

The total number of alarm messages received by the central console from this transponder since the data was last reset (using the **Reset Transponder Troubles** button).

Total Tests Received

The total number of test messages received by the central console from this transponder since the data was last reset (using the **Reset Transponder Troubles** button).

Total Troubles Processed

The total number of trouble messages received by the central console from the transponder and processed (see Total Troubles Shed) since the data was last reset (using the **Reset Transponder Troubles** button).

Total Troubles Shed

During certain rare occurrences, the communication traffic on the transponder links becomes excessive and threatens to increase the system response time to tests and alarms. This can happen if faults are reported at a very high rate. To avoid slow response in such situations, the central console may go into a load shedding mode in which it ceases to record and display Trouble Reports until the communications traffic subsides. The **Total Troubles Shed** box indicates the number of trouble messages that were not processed since the last reset (using **Reset Transponder Troubles** button).

Figure 433: Transponder Current

Successful Incoming Messages

The total number of messages successfully received from this transponder.

Incoming Format Errors

The number of messages received from this transponder where format error was detected. This field is yellow if 1.5% or more of the messages had errors. A high level of message errors indicates a serious communication problem.

Incoming Retried Messages

The total number of messages successfully received from this Transponder that indicated they were retried. This field is yellow if 1.5% or more of the messages are retried. A high level of retried messages indicates a serious communication problem.

Total Outgoing Messages

The total number of messages sent to this transponder from the central console.

Outgoing Retried Messages

The total number of message retries to this transponder. This field is yellow if 1.5% or more of the messages are retried. A high level of retried messages indicates a serious communication problem.

Outgoing Failed Messages

This is total number of messages that could not to be delivered to this transponder. This field is yellow if there are any failed messages. Outgoing failed messages cause the central console to display an alert message that communications have failed.

Stress Test

This checkbox causes the central console to continually request maps from the transponder. When in this mode, the central console sends a new map request as soon as it receives a map from the transponder, rotating through the map types. This test is used when diagnosing communications problems to create artificially high traffic on the communication link without interfering with the processing of alarms and tests. The stress test ceases when the checkbox is cleared, or this screen is closed by clicking the **Cancel** button.

Auto Scan

The auto scan function performs the above stress test proceeding from one transponder to the next after one of each type of map is requested and received. After the last map type and before proceeding to the next transponder, a command is issued to refresh the transponder data so that when an auto scan is proceeded through all transponders, all transponder and point troubles are updated. Auto scan is terminated by removing the check in the **Auto Scan** box or by closing the screen using the **Cancel** button.

Current Troubles

This window displays all current troubles for this transponder. In the Current Transponder Status Screen, there is a low battery and a tamper condition being reported for this transponder. This window also displays the restoration to a normal condition when it occurs. When the fault is corrected, clicking the **Acknowledge** button eliminates any Restoration Reports. Conditions, which were not rectified, remain in the window.

Not Responding Map

To assist in diagnosing problems with the receivers and alert units associated with a transponder, several commands can be issued from the central console to requesting information from the transponder. This button requests a map of all the devices on this transponder (receivers or alert units) that are not responding to the system. The current troubles list is automatically updated.

Jamming Map

This button requests a map of all the receivers on this transponder that are reporting a jamming condition to the system. The Current Troubles list is automatically updated.

Previous

Returns to the previous transponder.

Next

Advances to the next transponder.

Out of Service Map

This button requests a map of all devices on this transponder (receivers or alert units) that were manually taken out of service to the system. The current troubles list is automatically updated.

Tamper Map

This button requests a map of all the devices on this transponder (receivers or alert units) that are reporting a tamper condition to the system. The current troubles list is automatically updated.

Acknowledge

Clicking this button removes all restored troubles from the current troubles list.

AC Loss Map

This button requests a map of all the alert units on this transponder that are reporting an AC loss condition to the system. The current troubles list is automatically updated.

Refresh Data

Clicking this button updates all of the transponder level data in this screen. It does not update the device troubles (use stress test or auto scan to update the device troubles).

Reset Transponder Troubles

The **Reset Transponder Troubles** button is used to reset all of the alarm, test and message counters to zero, and to remove any restoration reports.

Low Battery Map

This button requests a map of all the alert units on this transponder that are reporting a low battery condition to the system. The current troubles list is automatically updated.

3.3.11 Transponder Parameter Change Screen

This screen allows parameters stored in the transponder's EEPROM memory to be viewed and changed.

Figure 444: Transponder Parameter Change Screen

Run Silent

If checked, the receivers and alert units on this transponder do not sound an alarm. This includes alarms received during a communications failure with the central console.

Optional Parameter

This is a future option, leave unchecked.

Loop Communications

When this option is checked, the communications to the transponders are wired in a loop. The output from the computer goes to the input of the first transponder. The output from the first transponder goes to the input of the second transponder, and so on until the output from the last transponder in the loop goes to the input of the computer. This form of communications allows fiber optic communications to be used (with third party fiber to RS-232 converters).

Enable Remote Key

If checked, the remote key supervised input on this transponder is enabled; otherwise, it is ignored.

Uses Proxim Radio

Only check this item if a Proxim radio is used to communicate to the central console.

Comm Fail to Siren Out

If this item is checked, the siren output on this transponder activates when a communications failure is detected at the central console.

Verbose Point Reports

If checked, alarm and test reports include average levels and packet count information. This extra information is for diagnostic purposes only and is not required for system operation. Since the additional data increases the system traffic load leave this item unchecked.

Test Min Level

This is the minimum receive level (1 to 255) a receiver must see before the green light displays acknowledging a successful test. Leave this item at default (128).

Test Differential

This is the minimum difference in receive level (1 to 255) a receiver must be less than the loudest receiver hearing a test before the green light displays acknowledging a successful test. Leave this item at default (64).

Alarm Min Level

This is the minimum receive level (1 to 255) a receiver must see before the sounder and red light is displayed for an alarm. Leave this item at default (1).

Alarm Differential

This is the minimum difference in receive level (1 to 255) a receiver must be less than the loudest receiver hearing an alarm before the sounder and red light are displayed for an alarm. Leave this item at default (255).

Byte

These are future options, leave at default (0).

Spare

This is a future option (leave unchecked).

Test Transmitter Type**Test Receiver 1****Test Receiver 1****Transmit Delay****Transmit Point****Load Delay****Tamper Load**

These parameters are used for engineering system load testing only.

Do not use in a live system, as they can generate more traffic than a system can handle; therefore, actual alarms may be missed. Leave them at default.

Transponder

Selects the transponder the data is presented for.

Previous

Returns to the previous transponder in the system.

Next

Advances to the next transponder in the system.

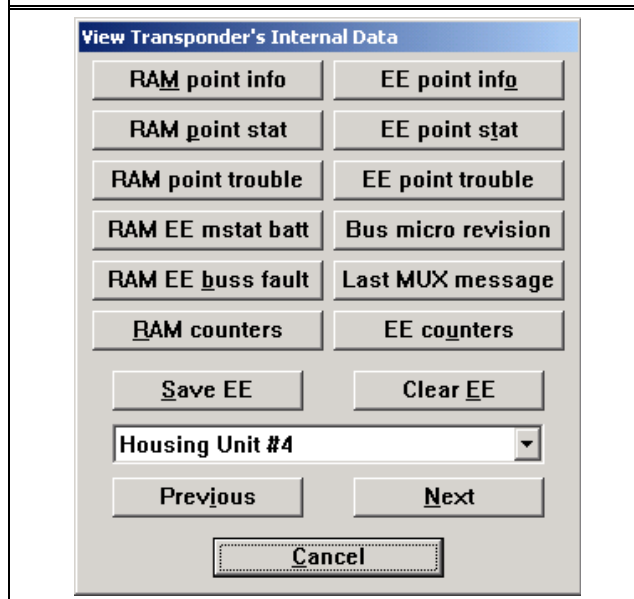
Send Change

Sends the changes made to the selected transponder. Changes are not made to the transponder EEPROM memory unless this button is clicked.

3.3.12 Transponder Data View Screen

This screen is for engineering evaluation of a transponder only.

Figure 455: Transponder Data View Screen



RAM Point Info

Views the RAM image of point information.

RAM Point Stat

Views the RAM image of point status.

RAM Point Trouble

Views the RAM image of point trouble.

RAM EE Mstat Batt

Views the RAM and EEPROM images of transponder status and battery condition.

RAM EE Buss Fault

Views the RAM and EEPROM images of transponder MUX bus fault condition.

RAM Counters

Views the RAM image of the process registers.

Save EE

Saves the current RAM image to the EEPROM memory on the transponder.

EE Point Info

Views the EEPROM image of point information.

EE Point Stat

Views the EEPROM image of point status.

EE Point Trouble

Views the EEPROM image of point trouble.

Bus Micro Revision

Views the bus micro revision for the connected points.

Last MUX Message

Views the last MUX bus message received.

EE counters

Views the EEPROM image of the process registers.

Clear EE

Clears the EEPROM memory on the transponder and resets the transponder.

Previous

Returns to the previous transponder in the system.

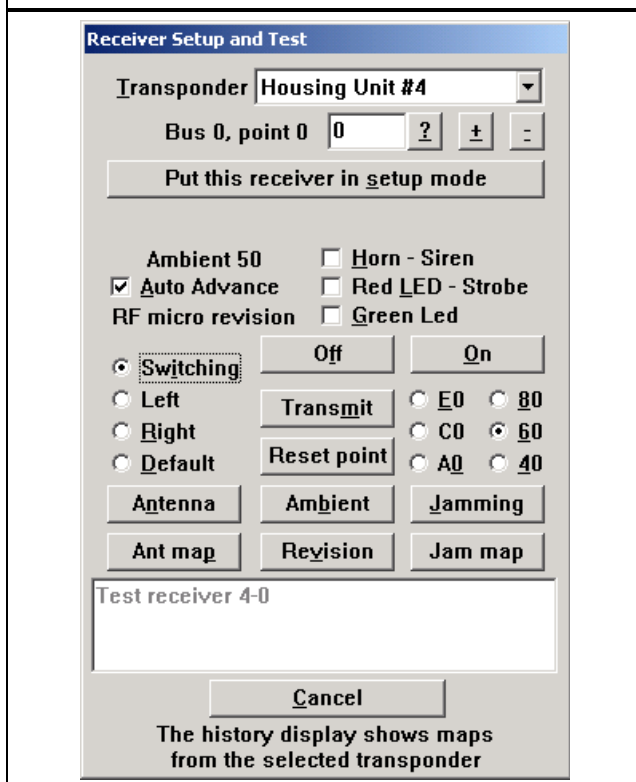
Next

Advances to the next transponder in the system.

3.3.13 Receiver Configuration Screen

Once the receiver and alert unit data for a transponder is entered into the Transponder Database, this screen is used to verify that each receiver is working and is properly addressed in the database. This setup tool identifies errors in the address switch settings of receivers and alert units, as well as data entry errors in the Transponder Database.

Figure 466: Receiver Configuration Screen



Put This Receiver In Setup Mode

This button initiates the setup process by causing both the red and green LED's of the selected receiver illuminate. The red and green LED flash. On the central console, the screen changes presenting an abort setup for this **MUX Point** button. This screen allows proceeding to the next device in the event that one receiver is not set up properly.

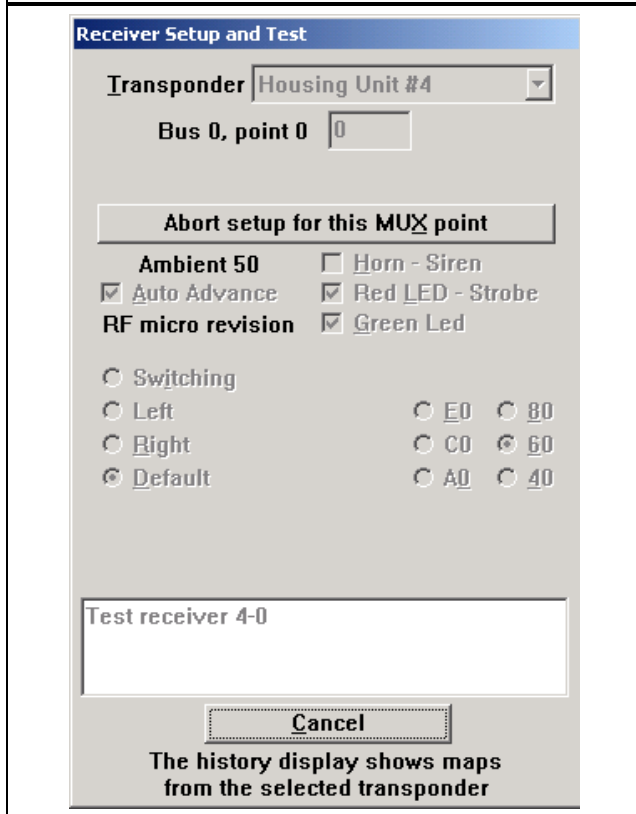
The next step is using a Maintenance Transmitter to transmit an alarm while standing near the receiver.

Note

The illuminated LED's indicate to the service person standing near the device that the receiver is actually the one currently in the setup mode. If the LED's of the designated receiver are not illuminated, there is probably an error in the switch settings of the receiver or an error in the address in the Transponder Database. To help resolve such problems, the person at the central console can command any device to illuminate its LED's and/or sound its horn.

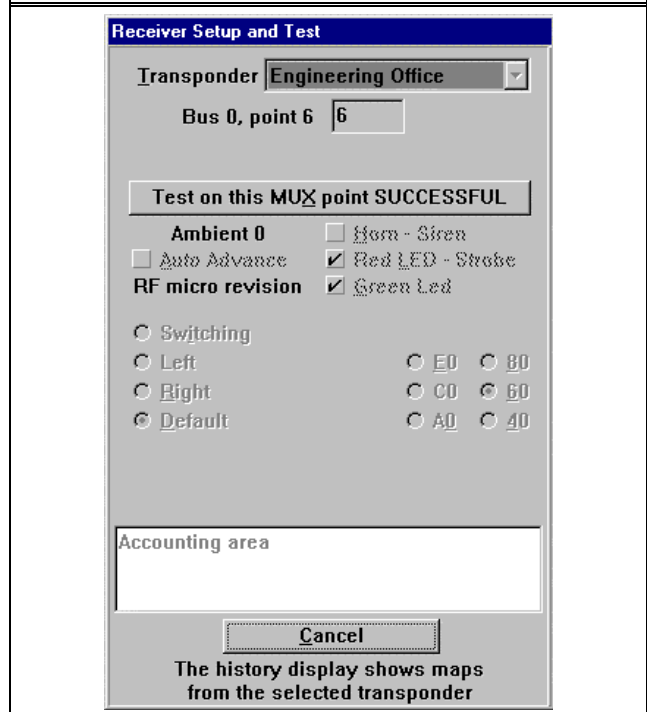
If the receiver in the Setup Mode detects the maintenance alarm and if the received signal is the strongest of all receivers, the horn on the receiver sounds briefly and the LED's go off. This indicates the receiver is functioning properly and the receiver's address is set correctly in the Transponder Database and on the receiver's switches.

Figure 477: Abort Button to Remove a Device from the Setup Mode



The central console also confirms the successful setup with an audible and text message. The **abort setup for this MUX Point** button disappears and is replaced by **Test On This MUX Point Successful** button. Click this button to conclude the test on this point (see Figure 48).

Figure 488: Confirmation of Successful Setup Test



Auto Advance

If this box is checked, the central console automatically selects the receiver with the next higher point address.

Horn - Siren

If this checkbox is checked, the horn output of a receiver or the siren output of an alert unit is turned on if **On** is clicked, or off if **Off** is clicked. If this checkbox is not checked, the state of this output does not change.

Green LED

If this checkbox is checked, the green LED output of a receiver or the spare output of an alert unit is turned on if **On** is clicked, or off if **Off** is clicked. If this checkbox is not checked, the state of this output does not change.

Red LED - Strobe

If this checkbox is checked, the red LED output of a receiver or the strobe output of an alert unit is turned on if **On** is clicked, or off if **Off** is clicked. If this checkbox is not checked, the state of this output does not change.

Off

When clicked, the checked **Horn-Siren**, **Green LED**, and **Red LED - Strobe** outputs are turned off for the selected point on the selected transponder. If the output does not change, click **On** and then click **Off** again.

On

When clicked, the checked **Horn-Siren**, **Green LED** and **Red LED - Strobe** outputs are turned on for the selected point on the selected transponder. If the output does not change, click **Off** and then click **On** again.

Ambient

The **Ambient** value is shown above **Auto Advance** displaying the current ambient level at the receiver. To get an updated ambient reading, select the point, click the **Transmit** button, and click the **Ambient** button.

RF Micro Version

The receiver's RF micro revision level is shown below **Auto Advance**. To get an updated reading, click the **Revision** button.

Antenna

Normally, a receiver automatically switches between its diversity antennas during normal operation (leave the default selection on a working system at this setting). The receiver can be forced to use only the left or right antenna, or always switch by selecting the appropriate setting and clicking the **Antenna** button.

Ant Map

Clicking **Ant Map** causes the system to interrogate the current antenna switching settings of all receivers on this transponder.

Transmit

Clicking **Transmit** causes this receiver to send one test transmission.

Reset Point

Clicking **Reset Point** causes the microprocessors on this point to reset as if they were just powered up. A receiver should not be reset in a working system, as it can cause receptions to be lost.

Ambient

Clicking **Ambient** causes the system to interrogate the current ambient levels of all receivers on this transponder.

Revision

Clicking **Revision** causes the system to interrogate the RF micro revision levels of all receivers on this transponder.

Jamming

A receiver monitors the ambient level during normal operation. If the ambient level rises above the jamming setting and jamming trouble, it is reported to the central console. The receiver's jamming level can be adjusted by selecting the appropriate setting (shown in hexadecimal levels) and clicking the **Jamming** button.

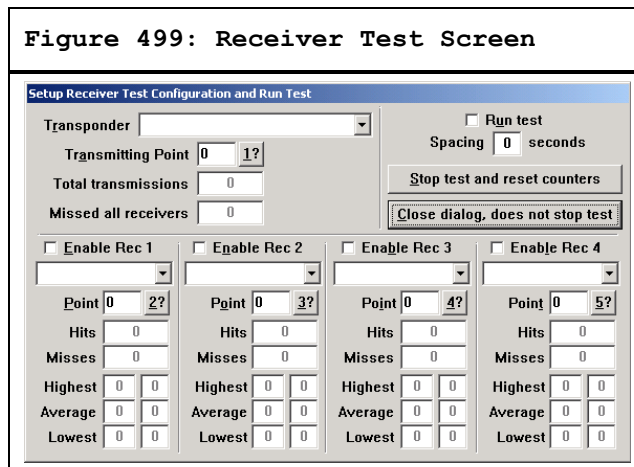
Jam Map

Clicking **Jam Map** causes the system to interrogate the jamming setting levels of all receivers on this transponder.

3.3.14 Receiver Test Screen

Use this screen to set up and monitor four receivers and listen to one receiver transmitting with its Buddy Check Transmitter. Normally, the function is for engineering evaluation of new transmitter and receiver designs, but it can be used to test receiver boards and locations in a working system.

Figure 499: Receiver Test Screen



Transponder

Select the transponder for the transmitting point and each receiving point. They can be on the same or different transponders.

Transmitting Point

Select the point (receiver) on the selected transponder to generate the transmissions.

Total Transmissions

The total number of times the designated receiver transmitted the test message.

Missed all Receivers

The total number of times that the test transmission, was not heard by any of the designated receivers.

Enable Rec

This box must be checked for this receiver to monitor the test transmissions.

Point

Select the point (receiver) on this transponder to monitor the test transmissions.

Hits

The number of times this receiver successfully heard the test transmission.

Misses

The number of times this receiver failed to hear the test transmission.

Highest

The left-hand box displays the highest receive level at which the test transmission was heard. The right-hand box displays the greatest number of packets heard from a single test transmission.

Average

The left-hand box displays the average receive level at which the test transmission was heard. The right-hand box displays the average number of packets heard from a single test transmission.

Lowest

The left-hand box displays the lowest receive level at which the test transmission was heard. The right-hand box displays the least number of packets heard from a single test transmission.

Run Test

The test only runs when this box is checked. To stop the test and retain the test values, uncheck this box.

Spacing

This slows the test by forcing this number of seconds between test transmissions. Normally, this setting is left at the default of 0.

Stop Test and Reset Counters

Clicking this button stops the test and resets all values.

Close Screen, Does Not Stop Test

Clicking this button closes this screen but does not stop the test from running. Reopening the screen displays the current progress of the test. The test should not be left running unless there is a specific need, as it generates both RF and system traffic.

3.3.15 Network Status Screen

This screen shows the status of communications on the network, modem, and system serial ports.

Figure 500: Network Status Screen

Current Serial Connection Network Status				
	Serial Network	Modem	Sys Serial 1	Sys Serial 2
Successful Incoming Messages	0	0	0	0
Incoming Communications Errors	0	0	0	0
Incoming Retried Messages	0	0	0	0
Total Outgoing Messages	0	0	0	0
Outgoing Retried Messages	0	0	0	0
Receive Buffer Max	0	0	0	0
Transmit Buffer Max	0	0	0	0
Buffer Overflow	0	0	0	0
Hardware Overrun	0	0	0	0
Total Remote Access Connections	0		Yellow indicates a problem	
Total Wrong Access Code Attempts	0		Reset Status	
Last Remote Access Time			Refresh Data	
Successful pager messages	0		Cancel	
Failed pager attempts	0			

Successful Incoming Messages

This value is the number of messages that the system successfully received on this communications port.

Incoming Communication Errors

This value is the number of messages that the system detected errors in, on this communications port. If displayed in yellow, this value is more than 1.5% of the Successful Incoming Messages.

Incoming Retried Messages

This value is number of successful receptions that indicated that they retried by the sending application. If displayed in yellow, this value is more than 1.5% of the Successful Incoming Messages.

Total Outgoing Messages

This value is total number of outgoing messages sent on this port.

Outgoing Retried Messages

This value is number of outgoing messages that were retried because the receiving application did not acknowledge them. If displayed in yellow, this value is more than 1.5% of the Total Outgoing Messages.

Receiver Buffer Max

This value is maximum number of bytes received on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.

Transmit Buffer Max

This value is maximum number of bytes processed by the system, but not yet transmitted on this serial port. If displayed in yellow, more than 50% of the queue was in use.

Buffer Overflow

This is the number of times a byte was lost by the software for a serial port because the input buffer overflowed. Bytes were placed into the input buffer faster than the system could process them.

Hardware Overrun

This is the number of times a byte was lost by the hardware for a serial port because it was not fast enough to process the byte into the input buffer.

Total Remote Access Connections

This value is the total number of times a remote access connection was successful.

Total Wrong Access Code Attempts

This value is the number of times a remote access connection was attempted and rejected because a valid remote access code was not received.

Last Remote Access Time

This is the time and date of the last successful remote access attempt.

Successful Pager Messages

This value is the number of successful pager messages sent.

Failed Pager Attempts

This value is the number of times a pager message dial-out was unsuccessful.

Reset Status

Pressing this button resets all values shown in this screen.

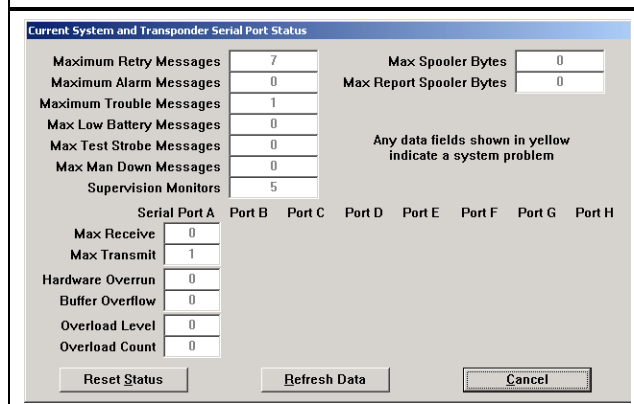
Refresh Data

Pressing this button refreshes all values shown in this screen. The values are not automatically updated when the screen is left open.

3.3.16 System Status Screen

This screen shows the status of internal system queues and communications on the serial ports assigned to transponders.

Figure 511: System Status Screen



Maximum Retry Messages

This value is maximum number of unacknowledged messages in queue to be sent to all transponders in the system. If displayed in yellow, more than 50% of the queue was in use at this value.

Maximum Alarm Messages

This value is the maximum number of alarms that the system processed at it busiest time. If displayed in yellow, more than 50% of the maximum was in use.

Maximum Trouble Messages

This value is the maximum number of troubles in the queue yet to be displayed. If displayed in yellow, more than 50% of the queue was in use.

Maximum Low Battery Messages

This value is the maximum number of transmitters with low batteries yet to be displayed. If displayed in yellow, more than 50% of the queue was in use.

Maximum Test Strobe Messages

This value is the maximum number of test strobes in use at one time. If displayed in yellow, more than 50% of the queue was in use.

Max Man Down Messages

This value is the maximum number of transmitters timing man down events, at one time. If displayed in yellow, more than 50% of the queue was in use.

Supervision Monitors

This value is the current number of transmitters being monitored for supervision transmissions.

Max Spooler Bytes

This value is the maximum number of bytes spooled for the printer at one time. If displayed in yellow, more than 50% of the queue was in use.

Max Report Spooler Bytes

This value is the maximum number of bytes spooled for the printer for Guard Tour Reports at one time. If displayed in yellow, more than 50% of the queue was in use.

Max Receiver Buffer

This value is the maximum number of bytes received from transponders on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.

Max Transmit Buffer

This value is the maximum number of bytes processed by the system, but not yet transmitted to the transponders on this serial port. If displayed in yellow, more than 50% of the queue was in use.

Hardware Overrun

This is the number of times a byte was lost by the hardware for a serial port because it was not fast enough to process the byte into the input buffer.

Buffer Overflow Count

This is the number of times a byte was lost by the software for a serial port because the input buffer overflowed. Bytes were placed into the input buffer faster than the system could process them.

Overload Level

This is a measure of the amount of time peak traffic on this serial port was greater than the system's ability to handle it. The system automatically sheds non-essential tasks when this value rises.

Overload Count

This is a measure of the number of times peak traffic on this serial port was greater than the system's ability to handle it. The system automatically sheds non-essential tasks when this value rises.

Reset Status

Pressing this button resets all values in this shown in this screen.

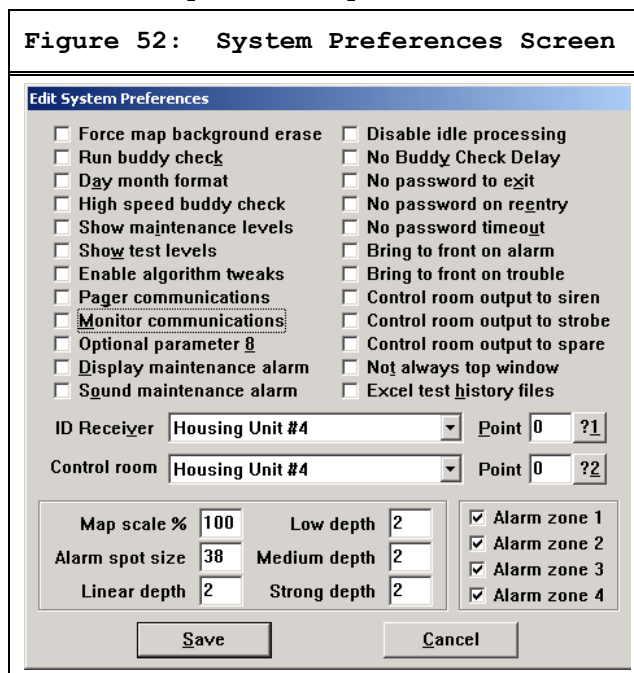
Refresh Data

Pressing this button refreshes all values shown in this screen. The values are not automatically updated when the screen is left open.

3.3.17 System Preferences Screen

The Set System Preferences Screen under the **Setup Menu** contains a number of settings that govern the behavior of the Security Escort System.

Figure 52: System Preferences Screen



Force Map Background Erase

Use this checkbox to erase the map screen. It should only be checked if there are problems with icons not being cleared properly from the screen; otherwise, it causes the screen to flicker.

Run Buddy Check

This checkbox enables and disables the buddy check feature of the system.

When checked, the central console periodically issues a command (by the transponders) to each receiver, to activate its on-board transmitter. The console then compares the signals received from neighboring receivers to the results of earlier buddy checks, identifying receivers that appear to have changed sensitivity.

Day Month Format

Checking this box causes all dates to be presented in day month year format rather than the month day year format used in North America.

High Speed Buddy Check

Checking this box allows the buddy check to run as fast as it can. Normally, only one buddy check transmission is sent each minute.

Show Maintenance Levels

Checking this box causes the central console to display the signal strength measured by each receiver as a number (from 1 to 15) inside the **Receiver** icon when maintenance alarms are displayed; otherwise, the floor number is displayed.

Show Test Levels

This checkbox causes signal strength levels to appear on the receiver icons when displaying tests on the Main Map Screen; otherwise, the green **Test** icons are displayed.

Enable Algorithm Tweaks

When checked, this checkbox causes the map scale, alarm spot size, and depth settings to be displayed in this screen. It also controls the display of the SA% and algorithm settings in the Transponder Edit Screen.

Pager Communications

Normally, this box is not checked. If checked, the communications to the dial-up wide area paging system through the modem displays on the History Screen. This function is only used to diagnose communications problems to the paging system.

Monitor Communications

Normally, this box is not checked. If checked, the communications to the modem displays on the History Screen. This function is only used to diagnose communications problems with the modem.

Display Maintenance Alarm

Normally, when a maintenance alarm is received from a maintenance transmitter the red light on all receivers hearing the transmission flashes for 5 seconds. If this box is checked, the receiver with the loudest reception level turns on both the red and green lights for 5 seconds.

Sound Maintenance Alarm

If this box is checked, the receiver with the loudest reception level on a maintenance alarm turns on its sounder for 5 seconds. Normally, this box is not checked.

Disable Idle Processing

Normally, this software registers with Windows to return to the Security Escort System if there is any idle time. The Security Escort System can use it to speed up its response to serial communications and other background tasks. If checked, the software is not registered for the idle time. Normally, this box is not checked. Windows NT and 2000 can show the amount of time each application (task) is taking. When this checkbox is not checked, it may appear that Security Escort System is hogging the processor resources. This is not true because the Security Escort System is only taking the time that Windows gives it through the idle process. To prove this, check this checkbox. The amount of time the Security Escort System needs drops dramatically and the Security Escort System continues to operate normally (same communications responses are slowed by several hundred milliseconds).

No Buddy Check Delay

If checked, the software does not impose the hour between buddy checks from the same receiver. Normally, this box is not checked and should not be checked for live systems.

No Password To Exit

If checked, the software exits without asking for a password. Normally, this box is not checked.

No Password on Reentry

If checked, the software does not ask for a password when the user switches to another program and then switches back to the still running Security Escort. Normally, this box is not checked.

No Password Timeout

If checked, the software does not ask for a password after the screen saver has run. Normally, this box is not checked.

Bring to Front on Alarm

If checked, the software jumps to the front when a new alarm occurs. Normally, this box is checked.

Bring to Front on Trouble

If checked, the software jumps to the front when a Trouble Screen pops-up. Normally, this box is checked.

Control Room Output to Siren

If checked, any time there is an unacknowledged alarm, the siren output on the Control Room Output indicated operates.

Control Room Output to Strobe

If checked, any time there is an unacknowledged alarm, the strobe output on the Control Room Output indicated operates.

Control Room Output to Spare

If checked, any time there is an unacknowledged alarm, the spare output on the Control Room Output operates.

Not Always Top Window

If the Security Escort System is intended to be the only application running on this computer, leave this checkbox unchecked. This prevents other applications from taking over the screen. Security Escort System is always present. If Security Escort System is to be run on a computer with other applications, check this box and Security Escort System shares the computer's display like all other Windows applications. After checking this box, stop and restart the Security Escort System for this feature to take effect. This checkbox is unchecked by default.

Excel Test History Files

Do not check this box in a live Security Escort System. It is for diagnostic engineering testing only.

Optional Parameter

These parameters are not currently used in the system. Leave unchecked.

ID Receiver - Assigning a Receiver For Automated Transmitter Exchanges

The Security Escort System contains a feature where the transmitter

identification number of a transmitter can be automatically entered into the Subscriber Database. This is used for entering transmitters when first issuing them to subscribers and for transmitter exchanges.

This automatic capture of the Transmitter Identification Number is accomplished by performing certain procedural steps (See the *Security Escort Operators Manual*) and then using the transmitter to make a test transmission in close proximity to a designated receiver, usually located close to the central console. By capturing the Transmitter Identification Number in this manner, keystroke errors are avoided during database entries and changes. The receiver chosen for this purpose is designated as the ID capture receiver. To assign the ID capture receiver, its transponder name and its point number are selected using the two boxes labeled transponder and point in the middle of the Set System Preferences Screen.

Control Room

The Security Escort System can activate an output to call attention when there is an alarm that was received and no operator responded to the system yet. To assign the control room output, select the Transponder Name it is connected to and its point number.

Alarm Zone

Four alarm zones allow the selection of which alarms from specific transmitters are reported on this workstation. This workstation displays the alarms only for the alarm zones that are checked. Each transmitter can be assigned to one or more alarm zones and when that transmitter generates an alarm (if this workstation has one or more of the same alarm zones checked), that alarm is displayed. The system defaults to all alarms displayed on all workstations.

Map Scale %'

This value changes the scale the maps are presented with. It is not intended for normal operations but is typically used for testing to allow more of the map to be seen. The setting may range from 30% to 400%. The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Alarm Spot Size

This setting changes the size of the yellow dot that marks the calculated location of the alarm. The settings range from 19 to 76 (half to double the default alarm dot size). It is best to set the size of the alarm spot so it represents a diameter of 15.24 m (50 ft.) on the displayed map (this is the area where the transmission of the alarm most likely took place). The **Enable Algorithm Tweaks** checkbox must be checked for this to be displayed.

Linear Depth

This setting controls the involvement of receivers in the alarm location calculation only when the Linear Algorithm is being used. The setting can range from zero to six (it defaults to two). When set to zero, only the receivers closer to the actual location of the alarm are considered in the location calculation. As the setting is raised, more distant receivers are included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the Linear Algorithm. The **Enable Algorithm Tweaks** checkbox must be checked for this to display.

Low Depth

This setting controls the involvement of receivers in the alarm location calculation only when the Low Algorithm is being used. The setting can range from zero to six (it defaults to two). When set to zero only, the receivers that are closer to the actual location of the alarm are considered in the location calculation. As the setting is raised, more distant receivers are included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the Low Algorithm. The **Enable Algorithm Tweaks** checkbox must be checked for this to display.

Medium Depth

This setting controls the involvement of receivers in the alarm location calculation only when the Medium Algorithm is being used. The setting can range from zero to six (it defaults to two). When set to zero only, the receivers that are closer to the actual location of the alarm considered in the location calculation. As the setting is raised, more distant receivers are included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the Medium Algorithm. The **Enable Algorithm Tweaks** checkbox must be checked for this to display.

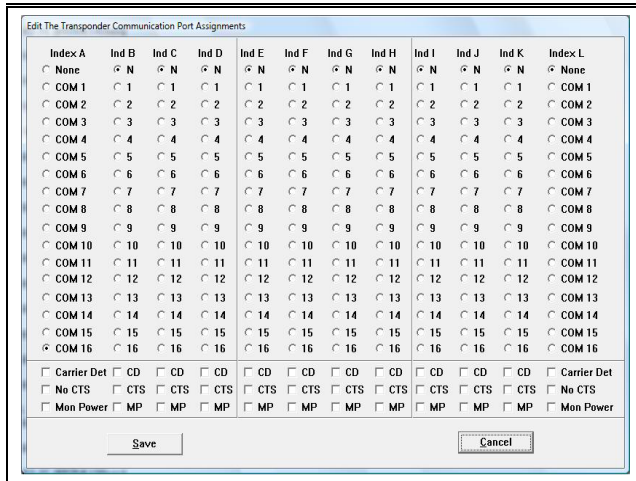
Strong Depth

This setting controls the involvement of receivers in the alarm location calculation only when the Strong Algorithm is being used. The setting can range from zero to six (it defaults to two). When set to zero only, the receivers that are closer to the actual location of the alarm are considered in the location calculation. As the setting is raised, more distant receivers are included in the alarm calculation. Typically, lower settings are better than higher settings. Change this setting if there are known problems with the location using the Strong Algorithm. The **Enable Algorithm Tweaks** checkbox must be checked for this to display.

3.3.18 Transponder Comm Port Setup Screen

This screen connects the Comm port indexes set for each transponder in the Transponder Database to the physical Comm ports on the computer.

Figure 533: Transponder Comm Port Setup Screen



COM

The actual physical Comm port over which communications to the transponder are carried.

Carrier Det

If checked, verify there is no carrier on the communications port before communicating. This setting is normally unchecked.

No CTS

If checked, do not monitor the "clear to send" before communicating. This setting is normally checked.

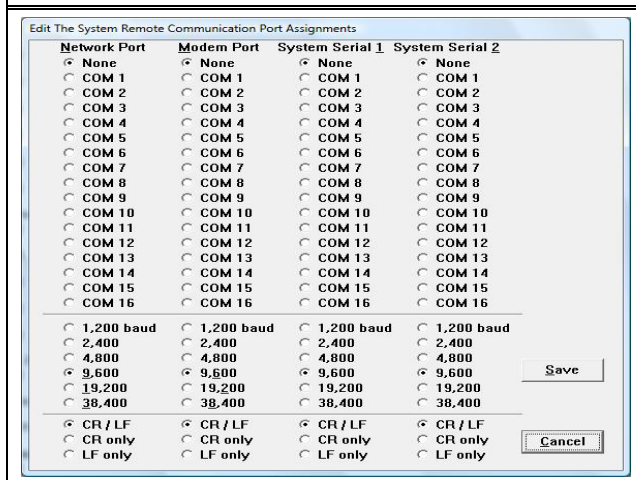
Mon Power

If checked, monitor the ring indicator pin to indicate a remote power supply used on this Comm link did not fail. This setting is normally unchecked.

3.3.19 Remote Comm Port Setup Screen

This screen connects the network, modem, and system serial ports to the physical Comm ports on the computer and sets their baud rate.

Figure 544: Remote Port Setup Screen



Network Port

This port connects the master and slave computers of the Security Escort System. If this system has only a single computer, this setting should be set to none.

Modem Port

This port typically connects to the modem for remote access and pager dial out.

If set in the Remote Setup Screen, use this port without a modem for direct connection to a computer that is always on line.

System Serial 1

This is a general-purpose serial port. Its function is set up in the Remote Setup Screen.

System Serial 2

This is a general-purpose serial port. Its function is set up in the Remote Setup Screen.

COM

The actual physical Comm port over which these communications are carried.

Baud

The speed at which characters are transmitted on this serial port. This setting must match the baud rate of the device connected at the other end of this serial connection. This setting should always be at the highest speed both connected devices have in common. Modem connections are typically much more efficient, if the baud rate is set significantly faster than the modems rated speed (for a 28.8 modem, set the baud rate to 57600 or 115200). The default setting is 9600 baud.

CR/LF

Appends carriage return and line feed characters at the end of each string transmitted (default). Only functions with the system serial ports (ignored on the network and modem ports).

CR Only

Appends a carriage return character at the end of each string transmitted. Only functions with the system serial ports (ignored on the network and modem ports).

LF Only

Appends a line feed character at the end of each string transmitted. Only functions with the system serial ports (ignored on the network and modem ports).

3.3.20 Remote Setup Screen

This screen sets up the remote access and system serial port parameters.

Figure 555: Remote Setup Screen
Default Master Computer

This computer is either the only computer in the system or on startup this computer defaults to the Master computer in a live Security Escort System.

Default Slave Computer

This computer, on startup, defaults to the slave computer in a live Security Escort System.

Workstation Computer

This computer is in a live Security Escort System. It can be used for all operator functions. It cannot control the system like the master and slave computers.

Remote Computer

This computer is not in a live Security Escort System. It is used only for remote access. For this setting to be enabled, all transponder Comm ports and the network port must be set to none.

Emergency Answer Only

Allows the master computer to answer a remote access only after ten rings. If the master does not answer, the slave answers after twelve rings.

Master Computer Answers

Allows the master computer to answer a remote access after the programmed number of rings. If the master does not answer, the slave answers after the programmed number of rings plus two.

Slave Computer Answers

Allows the slave computer to answer a remote access after the programmed number of rings. If the slave does not answer, the master answers after the programmed number of rings plus two. Generally, it is better to have the master computer answer remote access calls.

Direct Connect Port

The modem port is not connected to a modem. This setting allows a direct serial connection to another computer. This additional computer does not display alarms, but otherwise behaves like a slave computer.

Answering Machine Override

If checked, an answering machine is connected to this phone line. If the answering machine answers a remote access call, hang up and redial. When another call is received within 1 min. of the last ring of a previous call, the Security Escort System answers on the first ring, overriding the answering machine.

Pulse Dial

If checked, use pulse dial on all outgoing calls; otherwise, tone dialing (default) is used.

Answer On Ring

Program the number of rings on which to answer. If there is an answering machine on this phone line, set the number of rings to at least two greater than the number of rings the answering machine answers. Also check the **Answering Machine Override** checkbox.

Dialing Prefix

On outgoing calls enter the dialing prefix, if any.

Password

This is the password that is used to gain remote access to the Security Escort System. If the first five characters of the password match the remote systems password, read only access is allowed. If all twelve characters match, you can change system parameters remotely.

Password Verify

For verification, reenter the same password as above.

Disabled

If selected, this system serial port is disabled (default).

History Filter Output

If selected, this system serial port sends out whatever items are selected in the History Filter Screen.

Video Switcher Control

If selected, this system serial port sends out the strings programmed in the **Video Switcher** field of the Transponder Database Edit Screen's **Area** data. Also see Video Switcher Restore.

Remote System Control

If selected, this system is controlled by another system through a proprietary protocol. This setting can only be used when two systems are specifically designed to work together.

Video Switcher Restore

This string is output on any system serial port programmed for Video Switcher Control when all alarms are restored. This string is output to the video switcher to reset it to the default displays. Up to twenty characters can be entered. Control characters can be entered as [^][A] for control A.

Modem Init

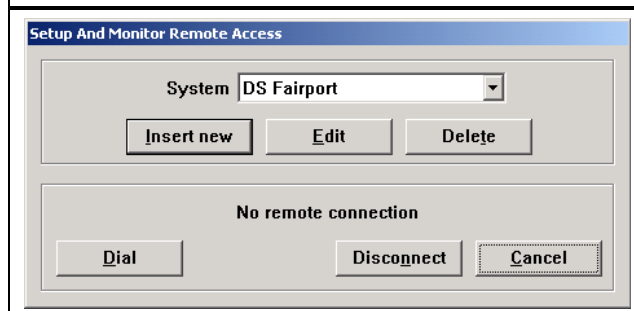
This is the initialization string output to the modem to set it up for all communications except paging. Normally, this setting does not need to change. To allow changes to this string, hold down the [SHIFT] and [CTRL] keys when this screen first opens. This string is specific to each modem model. The default string should work with most modems.

Modem Reset

This is the reset string output to the modem. Normally, this setting does not need to change. To allow changes to this string, hold down the [SHIFT] and [CTRL] keys when this screen is first opened. This string is specific to each modem model. The default string should work with most modems.

3.3.21 Remote Connection Screen

This screen sets up the remote access parameters that allow remote connection to a live Security Escort System.

Figure 566: Remote Connection Screen

Set the modem port and speed in the Remote Comm Port Setup Screen. The speed selected should be greater than the speed of the modem and the same as the speed selected for the remote system. Use the **Backup** command under the **Utilities Menu** to create a database backup to floppy. In the Remote Setup Screen, assign a password and set which computer (master or slave) is to answer and the number of rings to answer on. Also copy the map file from the live Security Escort System. The map is in the Escort sub-directory and is named MAP0.EDB. There also may be other maps under the names MAP1.EDB, MAP2.EDB, and so on.

In the Security Escort System used for remote access

This screen sets up the remote access parameters that allow remote connection to a live Security Escort System. Program all Comm port indexes in the Transponder Comm Port Setup Screen to none. In the Remote Comm Port Setup Screen, set the network port to none and set the modem to the Comm port of the modem. The speed selected should be greater than the speed of the modem and the same as the speed selected for the live system being called. In the Remote Setup Screen, set the master/slave/remote setting to remote. In the Remote Connection Screen select the **Insert** button and enter a name, password, phone number, and three-character file extension for this system's database files. Using a disk written with the **Backup** command of the system you desire access to, restore the database files. Select the system you just entered from the dropdown list box in the Remote Connection Screen. Exit the Remote Connection Screen and select Restore Screen under the **Utilities** Menu. Restore from the backup floppy to each databases. When done, you should also store a copy of the map file in the Escort sub-directory under the name MAP0.xxx, (where xxx is the three-character file extension entered earlier). After this is done, click **Dial** to call the remote system. If five, eight, or twelve characters of the password match, you can enter.

Insert New

Clicking this button presents a blank Phone Book Edit Screen to enter a new remote access Security Escort System.

Edit

Selecting the desired Security Escort System and then clicking this button allows the existing Security Escort System data to be edited.

Delete

Selecting the desired Security Escort System and then clicking this button deletes the data for the selected Security Escort System.

Dial

Selecting the desired Security Escort System and then clicking this button attempts to connect the selected Security Escort System. This selection is only available on the remote computer; it is not available on a live Security Escort system.

Answer

This option is only available in a live Security Escort System. Click this button manually answers an incoming call from a remote Security Escort System.

Disconnect

Clicking this button drops a remote connection. This can be done either on the live system or the remote access system.

Cancel

Clicking this button closes this screen but does not disconnect a remote access connection. At this point, you can navigate the menus and screens on the remote system as if you were at the on-site slave computer system. To drop the connection, return to this screen and click **Disconnect**.

3.3.22 Phone Book Edit Screen

This screen edits existing entries and adds new phone book entries for remote system access.

Figure 577: Phone Book Edit Screen

The screenshot shows a window titled "Edit Phone Book Database Record". It contains the following fields and values:

System name	DS Fairport
Phone number	716-223-4060
Access password	*****
Verify password	*****
3 Character system ID	DSF

At the bottom of the form are two buttons: "Save" and "Cancel".

System Name

This is a reference name for the Security Escort System to be accessed remotely. Use to select the desired system to be accessed in the Remote Connection Screen.

Phone Number

The phone number to be dialed to access the Security Escort System. Enter a comma for each 2 sec. pause desired.

Access Password

This is the password used to gain access to the remote Security Escort System. On the live system being dialed into, set the remote password in the Remote Setup Screen. If the first five characters of the password match, the remote system allows read only access. If all twelve characters match, you can change system parameters remotely.

Verify Password

For verification, retype the password entered into **Access Password**.

3 Character System ID

Enter a unique three character ID that is used as an extension to the map and database files for accessing this Security Escort System.

3.3.23 Pager Setup Screen

This screen sets up remote pager access for troubles (service) and alarms (security).

Figure 588: Pager Setup Screen

The screenshot shows a window titled "Set Up Pager Access - TAP or PET Pager Access Protocols". It is divided into two main sections: "Service pager" and "Security pager".

Service pager section:

- Automatically send selected troubles
- Select troubles in PopUp Trouble Filter
- Phone number: [text box]
- Password: [text box]
- Pager ID: [text box]
- Character limit: 80
- Pages per call: 4
- Pager group: [text box]
- 300 baud
- 1200 baud
- 9600 baud
- System name: [text box]
- System phone: [text box]

Security pager section:

- Send Installer demo alarms
- Send all other alarms
- Phone number: [text box]
- Password: [text box]
- Pager ID: [text box]
- Character limit: 80
- Pages per call: 4
- Pager group: [text box]
- 300 baud
- 1200 baud
- 9600 baud
- Security Pager Confm Not Reqd
- Cancel page if alarm reset
- Send page a second time, 2 minute delay
- Do not resend Alarm page

At the bottom, there is a "Modem init" field with the value "ATEM0VX&D2&Q", and "Save" and "Cancel" buttons.

Automatically Send Selected Troubles

If checked, send the troubles selected in the pop-up Trouble Filter Screen to the service pager.

Phone Number

Phone number to be dialed to access the paging service. This phone number is usually different from the number you manually dial to send a page. The paging company assigns this value.

Password

This is the password that must be sent to the paging service to send the page. If not required, leave this field blank. Usually a password is not required. The paging company assigns this value.

Pager ID

This is the ID that identifies the specific pager this message is to be sent to. Many times it is the last seven digits of the phone number you would manually dial to access this pager. The paging company assigns this value.

Character Limit

This is the maximum number of characters allowed per page. Typically, this is set to 80 characters. The Security Escort System truncates the pager message at this number of characters. The paging company assigns this value.

Pages Per Call

This is the maximum number of pager messages allowed per phone call. Typically, this is set to four pages per call. When this number of messages is sent and there are more messages to be delivered, the Security Escort System hangs up and redials the paging service to deliver the remaining messages. The paging company assigns this value.

Pager Group

This is the group of up to eight pagers this message is sent to. You can program the individual pager as well as a group of pagers. The pager group is sent the page before the individual.

Baud Rate

This is the baud rate used to communicate with the paging computers. The paging company assigns this value.

System Name

This identifies the Security Escort System when multiple Security Escort Systems report to the same service pager. Keep this field as short as possible since these characters, plus a space, are sent before each trouble message and are included in the character limit. If not desired, leave blank.

System Phone

This presents phone numbers to call in response to the service page. Only use if required since these characters, plus a space, are sent before each trouble message. They are included with the system name in the character limit. If not desired, leave blank.

Send Installer Demo Alarms

If checked, demo alarms are sent to the security pager.

Send All Other Alarms

If checked, all actual alarms are sent to the security pager.

Security Pager Confm Not Req'd

If checked, the confirmation pager message is not sent to the security pager when the alarm is acknowledged by an acknowledgement transmitter.

Cancel Page If Alarm Reset

If checked, the alarm page is canceled if the alarm is reset before it can be communicated to the paging service.

Send Page a Second Time, 2 Minute Delay

If checked, an alarm page is sent a second time to the security pager. Do this in case the pager was in an area where pages could not be heard when the first page was sent.

Do not resend Alarm page

If checked, a pager message is sent to the security person only once till the alarm is cancelled or acknowledged.

Modem Init

This is the initialization string sent to the modem to set it up for pager communications. Normally, this setting does not need to change. To allow changes to this string, hold down the [SHIFT] and [CTRL] keys when this screen first opens. This string is specific to each modem model. The default setting should work with most modems.

3.3.24 Send Pager Message Screen

Allows manually entered messages to be sent to the service or security pagers. Service and security pagers are configured in the Pager Setup Screen. Individuals and group pager assignments are set up in the Subscriber Database.

Figure 599: Send Pager Message Screen

Enter Text to be Sent

Enter the text to be sent to the pagers in the large text box at the top of the screen.

Send Service

Causes the entered message to be sent to the service pager and service pager group.

Send Security

Causes the entered message to be sent to the security pager and security pager group.

Stop all Pages

Causes all pages currently queued (automatic or manual) to be aborted and deleted. Use with caution.

Pager Group

To send a page to all members of a group, enter the pager group number here (1 to 99).

Send to Group

Click this button to send the text entered to the indicated pager group.

Select Individual

Use this drop down list to select an individual to page.

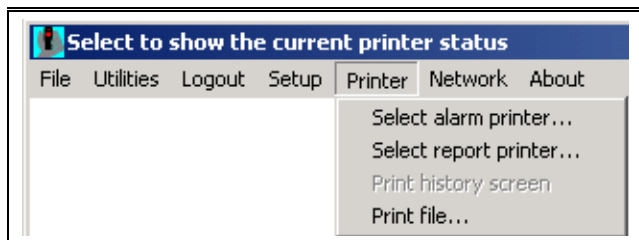
Send to Individual

Click this button to send the text entered to the indicated individual.

3.4 Printer Menu

The printer menu allows the alarm and report printers to be setup and enabled. You can also print the contents of the history screen and files.

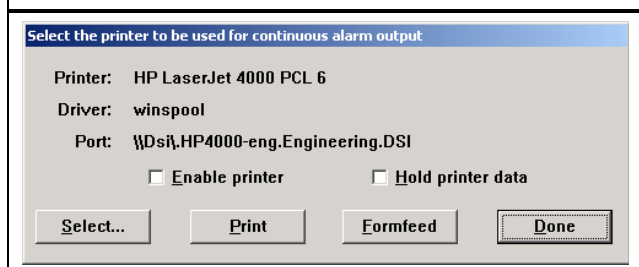
Figure 600: Printer menu



3.4.1 Select Alarm Printer Screen

The alarm printer is used to print all real time event data (alarm, tests, troubles and so on) as they happen. Typically, the alarm printer is a continuous form printer and not a page at a time printer such as a laser printer.

Figure 611: Alarm Printer Screen



Enable Printer

Check this checkbox to allow the system to send the real time events to the selected alarm printer.

Hold Printer Data

Check this checkbox to force the system to hold the data and not send it to the selected alarm printer. This is not recommended operation, but it allows a page at a time printer to be used as an alarm printer. Use the **Print** button to force the data to print on demand.

Select

Click this button to present the Window's System Printer Selection Screen. This screen is used to select the alarm printer from all of the printers that are installed on this computer.

Print

Click this button to print the data that is currently held in Security Escort's alarm printer buffer.

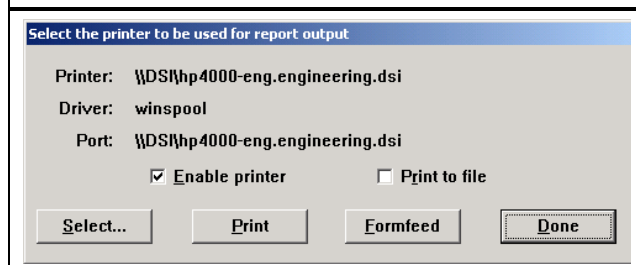
Formfeed

Click this button to send a formfeed to the alarm printer.

3.4.2 Select Report Printer Screen

The report printer is used to print all reports as they are requested automatically or by the operator. Typically, the report printer is a page at a time printer like a laser printer.

Figure 622: Report Printer Screen



Enable Printer

Check this checkbox to allow the system to send the reports to the selected report printer.

Print to File

Check this checkbox to create file copies of all reports. This option is independent of the report printer, which can also be used at the same time.

Select

Click this button to present the Window's System Printer Selection Screen. This screen is used to select the report printer from all of the printers that are installed on this computer.

Print

Click this button to print the data that is currently held in Security Escort's report printer buffer.

Formfeed

Click this button to send a formfeed to the report printer.

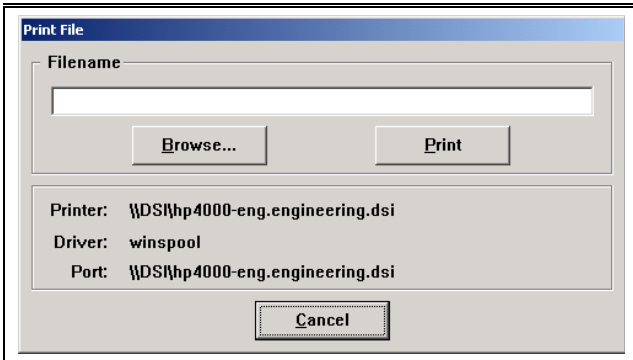
3.4.3 Print History Screen

This selection prints the current data in the History Screen buffer to the report printer.

3.4.4 Print File Screen

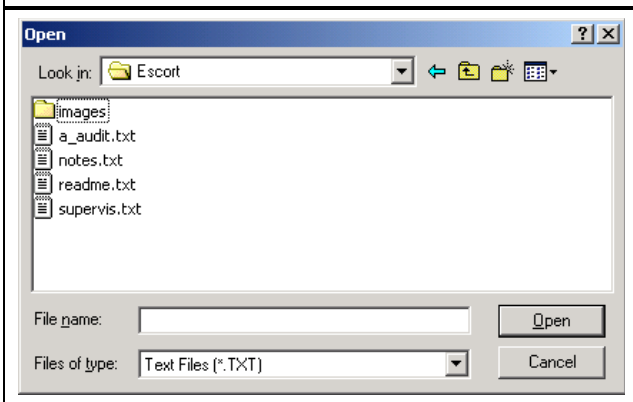
Enter the name of the file to be printed or click the **Browse** button to open the Common Open File Screen. Then click the **Print** button to print the file to the report printer.

Figure 633: Print File Screen



This is the standard Windows Common Open File Screen that is used for selecting the file to be printed. It works the same as any other Window's standard application.

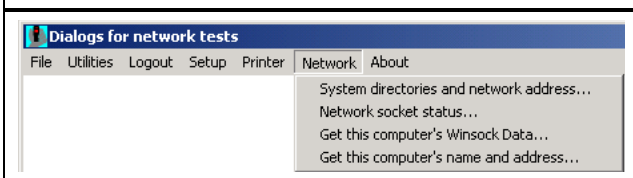
Figure 644: Common Open File Screen



3.5 Network Menu

This is the network menu used to set up and monitor the TCP/IP network and the computer's file paths.

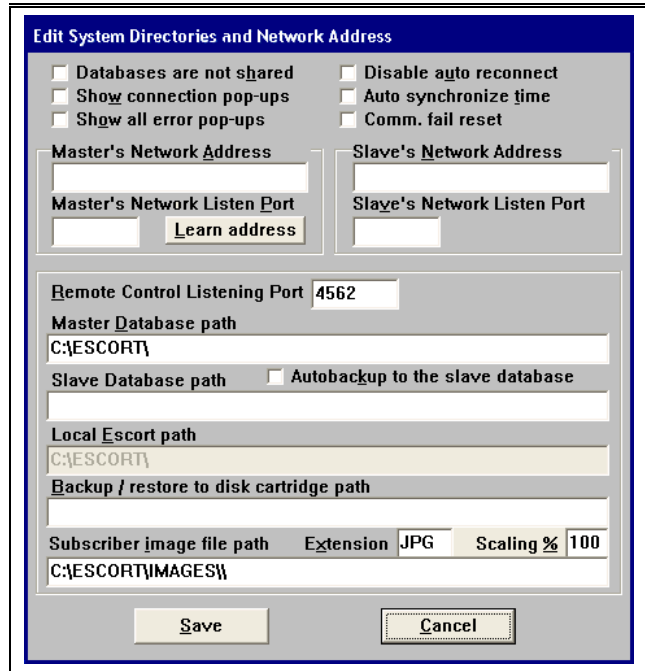
Figure 655: Network Menu



3.5.1 System Directories and Network Address Screen

Use this screen to set up the Network IP addresses and ports and related options. File paths can also be set up.

Figure 666: System Directories and Network Address Screen



Databases are not shared: If not checked, the master and all the slave and workstation computers share the same database files. This box must only be checked if each computer has its own copy of the databases stored locally. In normal operation, this box is typically unchecked. If this box is checked, the databases must be manually updated using backup and restore every time changes are made to the database.

Show connection pop-ups: If checked, shows a pop-up message box whenever a network connection is initiated or released with another computer. Unchecking this box stops the message boxes from displaying. In normal operation, this box is typically unchecked.

Show all error pop-ups: If checked, shows a pop-up message box whenever a network error is reported. Unchecking this box stops the message boxes from displaying. In normal operation, this box is typically unchecked.

Disable auto reconnect: If checked, the system does not automatically attempt to reconnect a lost connection each minute. Unchecking this box allows the system to automatically reconnect a lost connection. In normal operation, this box should be unchecked.

Auto synchronize time: If checked, the master computer automatically synchronizes the time on the slave and workstation computers once each night.

Option 6: This checkbox currently has no function and should be left unchecked.

Master's Network Address: The IP address of the master computer. There is no need to program the IP addresses of the workstation computers into the Security Escort software since they always establish the connection with the master and the slave. The Security Escort system requires a fixed IP address for the master computer.

Master's Network Listen Port: A unique number that indicates the Security Escort System software is attempting to set up a connection. Other software uses different port numbers, allowing the Network Interface Card to be shared with other network applications. Typically, this is set to 4561.

Learn address button. Clicking this button on the master computer automatically programs the master's IP address in the **Master's Network**

Address. If the computer has more than one Network Interface Card (NIC), you must verify the correct IP address was selected by comparing this address to the IP address that was programmed in the network control panel TCP/IP protocol for the master computer's network card. If the address is not correct, manually edit it to the IP address programmed in the network control panel TCP/IP protocol for the master computer's network card. Clicking this button on the slave computer automatically programs the slave's IP address in the **Slave's Network Address** field.

Slave's Network Address: The IP address of the slave computer. There is no need to program the IP addresses of the workstation computers into the Security Escort software since they always establish the connection with the master and the slave. The Security Escort System requires a fixed IP address for the optional slave computer.

Slave's Network Listen Port: A unique number that indicates the Security Escort software is attempting to set up a connection. Other software use different port numbers, allowing the NIC to be shared with other network applications. Typically, this is set to 4561.

Remote Control Listening Port

The Security Escort will be listening on this port to communicate with the OPC Server.

A separate OPC Server is created to communicate between the OPC Client and the Security Escort system. The OPC Server holds the alarm and trouble messages and sends the same to the available client once it is connected. The OPC server will send the status of the Security Escort to the OPC Client. The OPC sever also acknowledges and deletes alarm and trouble messages from OPC Client. If the connection between OPC Server and Security Escort goes down, the OPC server will try to reconnect with SE. Once the connection to the SE becomes active, the SE will send all the available alarms to the OPC server. The OPC server in turn sends the alarm back to OPC client; hence the OPC client may display some duplicate alarms.

Master Database Path: The path this slave or workstation computer uses to access the shared database files on the master computer. This path may have a different drive letter on the different slave and workstation computers. They are typically on the master computer but they may be on a file server or any other network accessible drive.

Note:

With version 2.04 of the software it is possible to use UNC path names rather than mapping drive letters. Therefore, the path to the master computer's database is [\\MASTER\C\ESCORT](#).

Autobackup to the slave database: If checked, the slave computer backs up all databases in the Master Database Path to the Slave Database Path each night at 3:00 AM.

Slave Database Path: The path this master or workstation computer uses to access the hot backup database files on the slave computer. This path may have a different drive letter on the different master and workstation computers. They are usually on the slave computer, but they may be on a file server or any other network accessible drive. Typically, they would not be stored on the same computer as the Master Database Path so a single failure would not prevent access to both the master and slave database files.

Note:

With version 2.04 of the software it is possible to use UNC path names rather than mapping drive letters. Therefore, the path to the master computer's database is [\\SLAVE\C\ESCORT](#).

Local Escort Path: The path on this workstation the Security Escort was installed in. Typically, it is C:\ESCORT.

Backup/Restore to Disk Cartridge Path

When backing up or restoring the databases to a disk cartridge use this path.

Subscriber Image File Path

The Security Escort System software can display an image for each subscriber on the alarm screen. This parameter tells the software the path to where the image files are stored. The default is C:\ESCORT\IMAGES.

Subscriber Image Extension

The subscriber images can be in JPEG or Windows Bitmap format. All images in a system must be in the same format. For the JPEG format, enter the Windows extension JPG. For the Bitmap format, enter the Windows extension BMP.

Subscriber Image Scaling %

When the display is set to 640 by 480 pixels and subscriber images are being displayed, this parameter controls the image size. This value can range from 10% to 100% and should be adjusted while viewing alarms to get the desired image size. When the display is set to 800 by 600 or larger (recommended), this parameter has no effect.

3.5.2 Network Socket Status Screen

This screen shows diagnostic information for the selected TCP/IP socket.

Figure 677: Current Network Socket Status Screen

Current Network Socket Status	
Socket number	1
IP address	Not connected
Port	None
Successful Incoming Messages	0
Incoming Communications Errors	0
Incoming Retried Messages	0
Total Outgoing Messages	0
Outgoing Retried Messages	0
Receive Buffer Max	0
Transmit Buffer Max	0
Yellow indicates a problem	
Previous	Reset Status
Next	Refresh Data
Cancel	

Successful Incoming Messages

This value is the number of messages the system successfully received on this socket.

Incoming Communication Errors

This value is the number of messages the system detected errors in, on this socket. If displayed in yellow, this value is more than 1.5% of the Successful Incoming Messages.

Incoming Retried Messages

This value is the number of successful receptions that indicated that the sending application retried. If displayed in yellow, this value is more than 1.5% of the Successful Incoming Messages.

Total Outgoing Messages

This value is the total number of outgoing messages that were sent on this socket.

Outgoing Retried Messages

This value is number of outgoing messages that must be retried because the receiving application did not acknowledge them. If displayed in yellow, this value is more than 1.5% of the Total Outgoing Messages.

Receive Buffer Max

This value is the maximum number of bytes that were received on this serial port, but not yet processed by the system. If displayed in yellow, more than 50% of the queue was in use.

Transmit Buffer Max

This value is the maximum number of bytes that were processed by the system, but not yet transmitted on this socket. If displayed in yellow, more than 50% of the queue was in use.

Reset Status

Pressing this button resets all values shown in this screen.

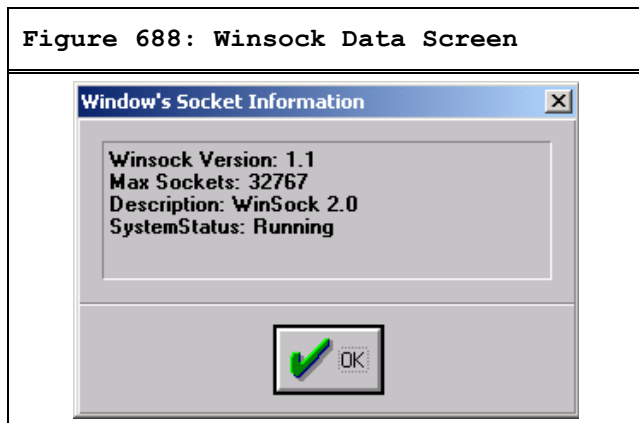
Refresh Data

Pressing this button refreshes all values shown in this screen. The values are not automatically updated when the screen is left open.

3.5.3 Winsock Data Screen

This screen shows information about the Windows Winsock support. This is only used for diagnostic purposes.

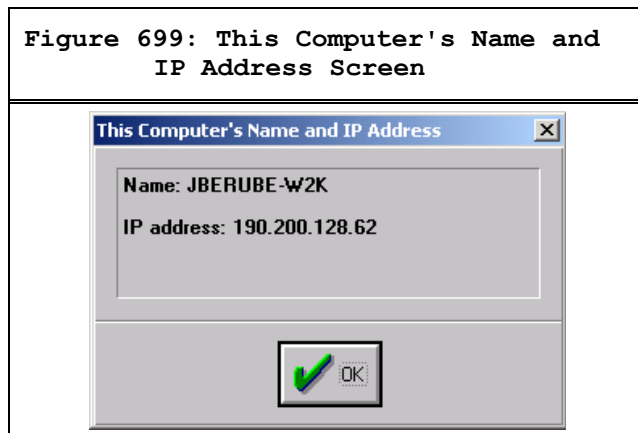
Figure 688: Winsock Data Screen



3.5.4 This Computer's Name and Address Screen

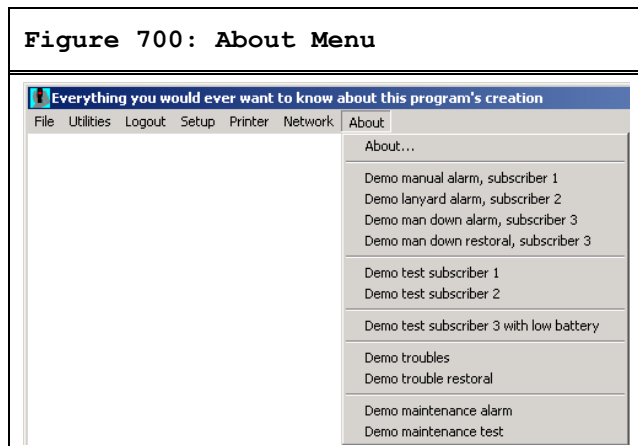
This screen show the computer's network name and current IP address.

Figure 699: This Computer's Name and IP Address Screen



3.6 About Menu

Figure 700: About Menu



Demo Manual Alarm, Subscriber 1

For demonstration only, it cannot be used in a live system. Causes the system to display an alarm from the subscriber with transmitter ID number one. In the System Preferences Screen, check **Enable Demo Selections** to enable these demo alarm and trouble selections. The transponder communication ports and network communication ports must also be disabled and the operator of the system must login at Installer or Installer Master authority level.

Demo Lanyard Alarm, Subscriber 2

For demonstration only, it cannot be used in a live system. Causes the system to display a lanyard alarm from the subscriber with transmitter ID number two.

Demo Man Down Alarm, Subscriber 3

For demonstration only, it cannot be used in a live system. Causes the system to display a man down alarm from the subscriber with transmitter ID number three. The man down alarm is delayed by the programmed man down delay (usually 10 seconds).

Demo Man Down Restoral, Subscriber 3

For demonstration only, it cannot be used in a live system. Restores a previous man down alarm from the subscriber with transmitter ID number two, if it has not timed out and is not being displayed.

Demo Test Subscriber 1

For demonstration only, it cannot be used in a live system. Simulates a test from the subscriber with transmitter ID number one.

Demo Test Subscriber 2

For demonstration only, it cannot be used in a live system. Simulates a test from the subscriber with transmitter ID number two.

Demo Test Subscriber 3 with low battery

For demonstration only, it cannot be used in a live system. Simulates a test from the subscriber with transmitter ID number three. This test also reports low battery.

Demo Troubles

For demonstration only, it cannot be used in a live system. Simulate troubles from a transponder. Point troubles are simulated for AC loss, tamper, and no response. Transponder troubles are simulated for remote key and remote key tamper. The individual troubles can be enabled or disabled in the pop-up Trouble Filter Screen. The trouble delay in the pop-up Trouble Filter Screen also affects these troubles. For demo purposes, it should be set to zero.

Demo Trouble Restoral

For demonstration only, it cannot be used in a live system. Simulates trouble restorals for all the troubles sent in Demo Troubles.

Demo Maintenance Alarm

For demonstration only, it cannot be used in a live system. Simulates an alarm from a maintenance transmitter.

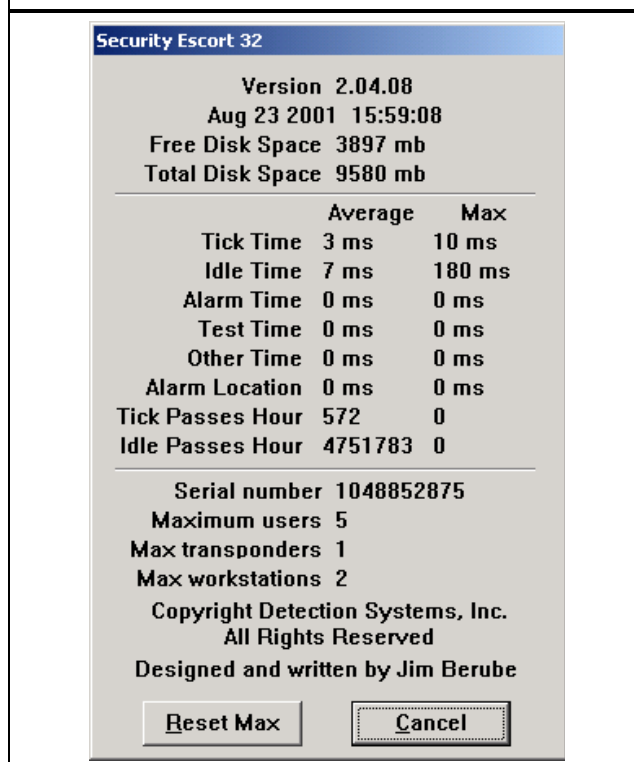
Demo Maintenance Test

For demonstration only, it cannot be used in a live system. Simulates a test from a maintenance transmitter.

3.6.1 About Screen

The About Screen presents the version information, copyright data, and internal processing timers.

Figure 711: About Screen



Software Version

At the top of the screen, the software version and the date and time that it was compiled is displayed.

Free Disk Space

This shows the free disk space on the "C" drive of this computer.

Total Disk Space

This shows the total disk space on the "C" drive of this computer.

Tick Time

The amount of time spent in the tick time processor per pass.

Idle Time

The amount of time spent in the Idle Time processor per pass.

Alarm Time

The amount of time spent to process each Alarm Report from a transponder.

Test Time

The amount of time spent to process each Test Report from a transponder.

Other Time

The amount of time spent to process each trouble and other message reports from a transponder.

Alarm Location

The amount of time spent to compute an alarm location.

Tick Passes Hour

The number of passes through the Tick Time processor that occurred in an hour.

Idle Passes Hour

The number of passes through the Idle Time processor that occurred in an hour.

Serial Number

Displays the serial number of this Security Escort System installation as read from the software key.

Maximum Users

Displays the maximum number of users this Security Escort System installation allows. This number is programmed into the software key.

Max Transponders

Displays the maximum number of transponders this Security Escort System installation allows. This number is programmed into the software key.

Max Workstations

Displays the maximum number of workstations this Security Escort System installation allows. This number is programmed into the software key.

Reset Max

Resets all of the max timers.

4.0 Files Required For Security Escort

The following files must be in the same directory as ESC32.EXE (default c:\escort):

- Esc32.exe: the main program
- Bwcc32.dll: support for the Screen appearance
- Cdrvd132.dll: communications support
- Cdrvhf32.dll: communications support
- Cdrvxf32.dll: communications support
- Comm32.dll: communications support
- W32mkde.exe: the database manager
- W32mkrc.dll: support for the database manager
- Wbtrcall.dll: support for the database manager
- Wbtrv32.dll: support for the database manager
- Lfbmp70n.dll: support for the screen images
- Lfcmp70n.dll: support for the screen images
- Ltkrn70n.dll: support for the screen images
- Ltfil70n.dll: support for the screen images
- Wprefers.edb the workstation preferences file
- The map of the facility is a standard Windows .BMP (bitmap) file. It must be stored in the same directory as ESC32.EXE and be named "Map0.edb."
- Map0.edb: map bitmap file

Note:

The following files are the system databases stored at the Master Database path:

- *Operator.edb: the System Operators Database*
- *Preferen.edb: System Preferences settings*
- *Reports.edb: Alarm Reports database*
- *Subscrib.edb: Database of the Subscribers/ Transmitters*

- *Transpon.edb: Database of the System Configuration*
- *Gpreferences.edb the Global Preferences file*

Note:

The following sound files should be in the Windows\media directory:

- *SEtroubl.wav: trouble sound*
- *SEalarm.wav: alarm sound*

Note:

These are sample images for demo and test. The following files should be in the \IMAGES directory, which is a sub-directory to the ESC32.EXE directory (default c:\escort\images):

- *Image1.jpg: sample subscriber image*
- *Image2.jpg: sample subscriber image*
- *Image3.jpg: sample subscriber image*

5.0 Image Files

5.1 Map File Generation and Scaling

The Security Escort maps are standard Windows bitmap files (.BMP). Map0.edb is the default map file, usually the ground floor in multiple map systems. The map must be saved in the Security Escort subdirectory (typically c:\Escort). These maps can be created from scratch using any Windows paint program; however, it is best to scan in an existing site map. Commercial copy centers usually have scanners that can handle larger drawing sizes.

If an AutoCad file is available, have AutoCad export a bitmap for the best looking maps that require the least work to make presentable. If the scale of the exported map is too large or too small, re-export the map at the corrected scale rather than scaling the map in a graphic editor. Scaling a bitmap file directly produces a file that requires a significant amount of manual effort to make presentable.

Save the scanned image as a Windows bitmap file (.BMP) with 256 colors (8 bit color). High Color (16 bit) or True Color (24 bit) can also be used, but the file sizes is much larger and the maps are slower to load and may require more system RAM. It should be scaled so that the entire map file is at least 800 by 600 pixels (covers the entire Windows screen). The Security Escort software auto scrolls the map; therefore, it is not a problem if the map is larger than the screen. The map should not be too large. There should be enough area of the map on the screen when an alarm is shown, so there is no question where in the facility the alarm is located from a quick review of the map. A good rule-of-thumb is 100 pixels represents 15.24 m (50 ft.) or greater.

5.2 Multiple Map Files

For a multi-story building, the maps for each floor must have the same resolution. Each map must be vertically aligned with all the floors above and below it. Therefore, the maps have the same origin (0,0 = upper left corner). Typically, you would do the map for the ground floor, then make the maps for the other floors by editing copies of the ground floor map.

Where transponders from multiple systems report into the same computer, the map(s) for each system is separate and assigned unique map numbers from the other maps on that same computer. The origin for the maps for each system is 0,0 = upper left corner. Therefore, the location of the receivers in the transponder database only consider this system's map without respect to the maps for any other systems being handled by the same computer.

The maps must be named Map0.edb, Map1.edb through Map99.edb. Where Map0.edb is the default map file, usually the ground floor. The Security Escort software shows the default map if there is no other events being processed at a given time.

Assign the desired map number to an area or point in the transponder database. Assign the map for a fixed location transmitters in the Subscriber Database Advanced Screen.

5.3 Subscriber Images

Display subscriber images. This software does not capture the subscriber images; it displays images that were previously captured by some other means. The subscriber image can be captured using a digital camera, video capture board and so on. The source of the image is not critical. We have not identified, nor do we require a specific manufacturer of the image capture equipment. The images must be saved individually in JPG format. The images should not be larger than 160 pixels wide and 160 pixels high. If they are, they are scaled and therefore they may lose image quality. Under the **Setup Menu** in the System Preferences

Screen the path to the images is set in subscriber image file path (default location of the images is "C:\ESCORT\IMAGES", but they can be located anywhere). The three-character file extension of the image files is set in Extension (default is JPG). Subscriber images can also be saved in Windows bitmap (.BMP); however, this format requires significantly more disk storage.

Only when the display is set to 640 by 480 (not recommended) the images display on top of the map and the Scaling % (10 to 200) controls the size of the image (try different settings to control the image size in the alarm screen). Under the **Files Menu** in the Subscriber Database Screen, select the desired subscriber and click **Edit data**. The image file is the name of file that has this subscriber's image. For example, if the subscriber's image is stored in a file with the name Image1.jpg, enter **Image1** in this box. You should have a minimum of a 1 MB video card to display subscriber's images. Go to the **Windows 95 (Windows 98, Windows NT) Task bar** and click the **Start** button. Select **Settings → Control panel → Display**. Click the **Settings** tab. In the **Color palette** control you can select 256 color, High Color (16 bit) or True Color (24 bit). Set the system to High Color or True Color (256 color is likely to produce undesirable results). When in doubt, set to High Color. In the same screen, **Desktop area** can be set to 640 by 480, 800 by 600, or 1024 by 768 pixels. When the display is set to 640 by 480 (not recommended), the images are displayed on top of the map and therefore limit how much of the map displays. The 1024 by 768 setting may require too much memory for most video cards and show more of the map, decreasing the size of the map details. Most video cards can be set to 800 by 600 and when in doubt this setting should be selected. If you cannot choose these settings, your video card or monitor setting may be incorrect, refer to the system documentation to correct.

6.0 Security Escort Pager Setup

With version 1.10 and higher, Security Escort supports:

- Up to 256 individual alphanumeric pagers; grouped into 99 groups of eight.
- Both dial up and local serial port connected paging systems, in the same system, at the same time.
- Service pages that can activate a group of eight service pagers in addition to a single pager.
- Alarm pages that can activate a group of eight alarm pagers in addition to a single pager. All alarms located in an alarm area can page an additional group of eight pagers specific to that area.
- Manual pages sent to any individual pager or pager group.
- All paging system communication using the TAP or PET protocols. This is true for both the dial-up and local serial port connected paging systems. Currently there is no support for any other pager protocols.

The system does not support numeric only or vibrate only pagers.

At this time, the only local paging system tested is TEKK model: PT-400 (Tekk Inc., 226 N. W. Parkway, Kansas City, MO, Phone (816) 746-1098, Fax (816) 746-1093).

Set the DIP switch for TAP Mode, 9600N81, Switch 6 off, all other switches on.

The pager ID to be used for each pager is the seven-digit CAP code that is on a label on the back of the pager (such as 0991001). A three-digit code must be appended to the end of the CAP code. For example, 0991001ERF where E is the Message Encoding Type, R is the RF data rate, and F is the Function Code.

Message Encoding Type (E) must be a "1" for alphanumeric coding.

RF data rate (R) is "5" for 512 BPS, "1" for 1200 BPS, or "2" for 2400 BPS. Many systems use 512 BPS for more reliable transmissions.

Function Code (F) may be set to one through four for a specific function code or zero for the default (recommend the Function Code be set to zero).

For an alphanumeric pager communicating at 512 BPS, the pager ID in our example is 0991001150.

For dial-up paging systems, the paging company assigns the phone number and Pager ID. Typically, the pager ID is the last seven digits dialed to access the pager from a phone.

Service pages page the members of the service group first, followed by the single service pager.

Alarm pages page the members of the alarm area paging group first (if any), followed by the alarm group, and finally the single alarm pager.

6.1 Dial-up Paging Modem Setup

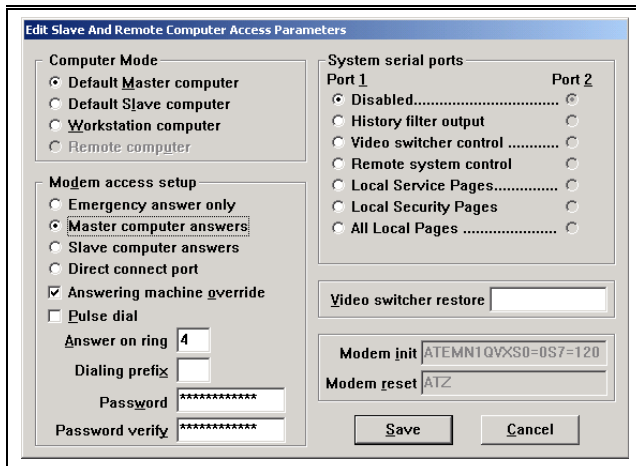
All dial-up pager access is through the modem. The baud rate set up in the Remote Comm Port Setup Screen under the **Setup Menu** for the modem port is for remote access to the Security Escort System and not for pager dial-up access. Leave this baud rate at the correct setting for remote access.

6.2 Local Paging Setup

The local paging system is accessed through a system serial port. **Assign System Serial Port 1 or 2** to the computer port to be used in the Remote Comm Port Setup Screen under the **Setup Menu**. Also configure the baud rate to match the local paging system (typically 9600 baud).

In the Remote Setup Screen, assign **System Serial Port 1 or 2** as the destination for **Local Service Pages**, **Local Security Pages**, or **All Local Pages**.

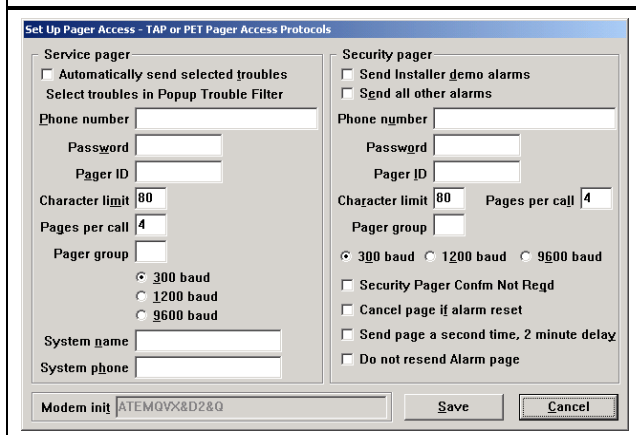
Figure 722: Remote Setup Screen



6.3 Service and Security (Alarm) Pager Setup

Pager access is setup in the Pager Setup Screen under the **Setup Menu**. Refer to the Pager Setup Screen for the details not covered here.

Figure 733: Pager Setup Screen



For both the service and security pagers, an individual pager (phone number, password, and pager ID) can be assigned. The pager ID is required for all individual pagers, dial-up and local. If the phone number and password are assigned, the page is sent over the modem connection. If the phone number and password fields are both blank, the page is routed to the local paging system. If you do not desire an individual pager, leave the phone number, password, and pager ID fields blank.

Both the service and security pagers also support paging groups. If a group number is programmed in the pager group field, all the members of that group are paged for every service or alarm page.

If service or alarm pages are enabled, either the paging group or individual pager must be filled in. They may both be filled in if desired.

The baud rate assignments in this screen affect only the dial-up paging access through the modem (get the desired baud rate from the paging company). These baud rate selections have no effect on local paging systems or remote system access. Remember that dial-up pages may be routed to different paging companies and they may require different baud rates. Set the baud rate to the highest baud rate common to all of the paging companies to be accessed.

The character limit (characters per page), pages per call affect all pages of the indicated type (local and dial-up). These fields must be set to the lowest setting for any of the routes that may be used. Remember that dial-up pages may be routed to different paging companies and they may have different restrictions.


6.4 Subscriber (Individual) Pager Setup

In the Subscriber Database, select the record for the desired individual. Press **Edit data** then press **Advanced**. The screen displays.

The pager ID is required for all individual pagers dial-up and local. If the phone number and password are assigned, the page is sent over the modem connection. If the phone number and password fields are blank, the page is routed to the local paging system. If you do not desire this individual to have pager support, leave the phone number, password, and pager ID fields blank.

Figure 744: Subscriber Database Advanced Screen

If the pager information is entered, this individual may be assigned to three paging groups. Each group accepts eight members maximum. Remember, it takes time to communicate with a paging service; therefore, only add members to a group if they need to be there. Otherwise, you may slow the paging report to people that must respond.



A pager group may contain members accessed by the local paging system and members that require dial-up access. Dial-up access typically takes much longer and it may slow pages to the local paging system.

6.5 Alarm Area Setup

In the Transponder Database under the **File Menu**, select the transponder with the desired programmed alarm area. Then click **Edit data**. Click **Show areas** and select the area desired.

The pager group field may be programmed with a pager group that is paged if this area is the most likely location of an alarm. This pager group is the first group paged to allow quick response by those individuals charged with responding to an alarm in this area. Each area may be assigned a pager group that can be the same or different from other alarm areas.

Figure 755: Transponder Area Edit Screen

The default alarm pager group defined in the Pager Setup Screen is paged after the pager group assigned to an area. If a pager group is not assigned to an area or the alarm location is not within a defined area, only the default pager group is paged.

6.6 Manual Pages

Select the Send Pager Message Screen under the **Setup Menu** to send manual pages.

Type the desired message in the large text box on the top.

- To send the page to all members of the default service pager group, click **Send Service**.
- To send the page to all members of the default security pager group, click **Send Security**.
- To send the page to all members of a specific pager group, enter the desired group number in the pager group field and click **Send to group**.
- To send the page to an individual, click the down arrow to display a list of the individuals that are programmed in this system. Select the desired individual by clicking on their name with the left mouse button, then click **Send to individual**.

Figure 766: Send a Pager Text Message Screen

Send A Pager Text Message

Insert the text to be sent here.

Enter pager text and select the desired individual or group

Send Service Send Security Stop all pages Cancel

Pager group Send to group

Send to individual

7.0 Importing a Subscriber Database

This section describes the file format required to import data into the Subscriber Database. There is no way to undo this operation, therefore, **DO A DATABASE BACKUP FIRST** and verify the updated data before the changed database is placed in service. If there are problems, restore the Subscriber Database from the backup.

The file of new data record entries must be in tab delimited text format. It must be placed in the Security Escort subdirectory (typically C:\Escort) and be named TABMERGE.DAT. The data fields must be in the following order, delimited by the horizontal tab character (decimal 8), and the record must be terminated with a carriage return (decimal 13). If a data field has no data, store the terminating tab character for that field. The total number of characters in all the fields of a record must be 255 characters or less, including the tab and carriage return characters. After the TABMERGE.DAT file is stored in the Security Escort subdirectory, start ESC32.EXE, enter the Subscriber Database, and click the **DATA MERGE** button. Be patient, it may take a while. Watch for the disk activity to stop. After the data is successfully merged, it is a good idea to remove the TABMERGE.DAT file to disable the DATA MERGE feature.

Table 1: Importing a Subscriber Database

Data Fields in Required Order	Excel Column	Restrictions
Subscriber Name	A	This field can be up to 30 characters. This field can contain any printable ASCII character except the "?".
Subscriber ID	B	This field can be up to twelve characters. This field can contain only ALPHA, numeric and the dash ASCII characters.
Home Phone Number	C	This field can be up to sixteen characters. This field can contain only numeric, "#", "*", "(", ")", comma and the dash ASCII characters.
Home Address 1	D	This field can be up to 30 characters. This field can contain any printable ASCII character except the "?".
Home Address 2	E	This field can be up to 30 characters. This field can contain any printable ASCII character except the "?".
Home City	F	This field can be up to twenty characters. This field can contain any printable ASCII character except the "?".
Home State	G	This field can be up to three characters. This field can contain only ALPHA ASCII characters.
Home Zip	H	This field can be up to ten characters. This field can contain only ALPHA, numeric and the dash ASCII characters.
Away Phone Number	I	This field can be up to sixteen characters. This field can contain only numeric, "#", "*", "(", ")", comma and the dash ASCII characters.
Away Address 1	J	This field can be up to 30 characters. This field can contain any printable ASCII character except the "?".
Away Address 2	K	This field can be up to 30 characters. This field can contain any printable ASCII character except the "?".
Away City	L	This field can be up to twenty characters. This field can contain any printable ASCII character except the "?".
Away State	M	This field can be up to 3 characters. This field can contain only ALPHA ASCII characters.
Away Zip	N	This field can be up to 10 characters. This field can contain only ALPHA, numeric and the dash ASCII characters.
Supplemental Text Field 1	O	This field can be up to 254 characters. This field can contain any printable ASCII character except the "?".
Supplemental Text Field 2	P	This field can be up to 254 characters. This field can contain any printable ASCII character except the "?".
Supplemental Text Field 3	Q	This field can be up to 254 characters. This field can contain any printable ASCII character except the "?".
Supplemental Text Field 4	R	This field can be up to 254 characters. This field can contain any printable ASCII character except the "?".
Pager Phone Number	S	This field can be up to 16 characters. This field can contain only numeric, "#", "*", "(", ")", comma and the dash ASCII characters.
Pager Password	T	This field can be up to 6 characters. This field can contain only numeric, and ALPHA ASCII characters.
Pager Pager ID	U	This field can be up to 10 characters. This field can contain only numeric ASCII characters.
Subscriber Type	V	0 Unclassified, 1 Commuter, 2 Faculty, 3 Resident, 4 Security, 5 Staff, 6 Installer, 7 Out of Service, 8 Watchman, 9 Visitor, 10 Point type, 11 Acknowledgement. This field should contain only numeric ASCII characters.
Handicapped Type	W	0 No handicap, 1 Blind, 2 Deaf, 3 Handicapped, 4 Wheel chair. This field should contain only numeric ASCII characters.
Transmitter ID	X	This field may be up to 9 characters. This field should contain only numeric ASCII characters.
Away Name	Y	This field can be up to 30 characters. This field can contain any printable ASCII character except the "?".
Image Filename	Z	This field can be up to 30 characters. This field can contain any printable ASCII character that is valid for a file name.
Height Feet	AA	0-7, This field should contain only numeric ASCII characters.
Height Inches	AB	0-11, This field should contain only numeric ASCII characters.

Table 1: continued

Data Fields in Required Order	Excel Column	Restrictions
Build Code	AC	0 Medium, 1 Slim, 2 Large. This field should contain only numeric ASCII characters.
Hair Color	AD	0 Brown, 1 Auburn, 2 Black, 3 Blond, 4 Brunet, 5 Grey, 6 Red. This field should contain only numeric ASCII characters.
Eye Color	AE	0 Brown, 1 Blue, 2 Green, 3 Hazel, 4 Grey. This field should contain only numeric ASCII characters.
Pager Group A	AF	0-99, This field should contain only numeric ASCII characters.
Pager Group B	AG	0-99, This field should contain only numeric ASCII characters.
Pager Group C	AH	0-99, This field may contain only numeric ASCII characters.
Fixed Floor Level	AI	0 Basement5, 1 Basement4, 2 Basement3, 3 Basement2, 4 Basement1, 5 Tunnel, 6 Basement, 7 Ground, 8 Outside, 9 Floor 1, 10 Floor 2, 11 Floor 3, 12 Floor 4, 13 Floor 5, 14 Floor 6, 15 Floor 7, 16 Floor 8, 17 Floor 9, 18 Floor 10, 19 Floor 11, 20 Floor 12, 21 Floor 13, 22 Floor 14, 23 Floor 15, 24 Floor 16, 25 Floor 17, 26 Floor 18, 27 Floor 19, 28 Floor 20, 29 Floor 21, 30 Floor 22, 31 Floor 23, 32 Floor 24, 33 Floor 25, 34 Floor 26, 35 Floor 27, 36 Floor 28, 37 Floor 29, 38 Floor 30, 39 Floor 31, 40 Floor 32, 41 Floor 33, 42 Floor 34, 43 Floor 35, 44 Floor 36, 45 Floor 37, 46 Floor 38, 47 Floor 39. This field should contain only numeric ASCII characters.
Fixed Map X Location	AJ	This field can contain only numeric ASCII characters.
Fixed Map Y Location	AK	This field can contain only numeric ASCII characters.
Fixed Bitmap Number	AL	0-99 This field can contain only numeric ASCII characters.
Supervision Interval	AM	0 None, 1 is 90 Second Supervision, 2 is 30 Second Supervision, 3 is 1 Hour Supervision. This field can contain only numeric ASCII characters.
Alarm Group	AN	0-99, This field can contain only numeric ASCII characters.
Shorted Loop	AO	This field can contain only numeric ASCII characters.
Open Loop	AP	This field can contain only numeric ASCII characters.
Status	AQ	Encoded value. Do not change.
Enable Magnetic Reed	AR	This field can contain only numeric ASCII characters.
Fixed Location Text	AS	This field can be up to 254 characters. This field can contain any printable ASCII character except the "?".
Magnetic Reed Text	AT	This field can be up to 30 characters. This field can contain any printable ASCII character except the "?".
Shorted Loop Text	AU	This field can be up to 30 characters. This field can contain any printable ASCII character except the "?".
Open Loop Text	AV	This field can be up to 30 characters. This field can contain any printable ASCII character except the "?".
Status Flags	AW	Encoded value. Do not change.
Modify Op	AX	0-30000, this field can contain only numeric ASCII characters.
Test Time	AY	Encoded 32-bit time value. Do not change.
Last Transmitter Change	AZ	Encoded 32-bit time value. Do not change.
Spare Date	BA	Encoded 32-bit time value. Do not change.
Last Fail To Test Letter	BB	Encoded 32-bit time value. Do not change.
Created	BC	Encoded 32-bit time value. Do not change.
Modified	BD	Encoded 32-bit time value. Do not change.
Low Battery	BE	Encoded 32-bit time value. Do not change.
Spare2	BF	This field should be blank.
Spare3	BG	This field should be blank.
Spare4	BH	This field should be blank.
Spare5	BI	This field should be blank.
Number Of Tests	BJ	This field may contain only numeric ASCII characters.

3

3 Character System ID62

A

Abort setup for this MUX Point50
 About menu68
 About Screen69
 AC Loss40, 41, 43
 AC Loss Map47
 Access Password62
 Acknowledge36, 47
 Add34
 Alarm56
 Central Console response to11
 Central Console screen display of11
 Maintenance14
 Multiple, simultaneous12
 Sequence of occurrences10
 Alarm Differential48
 Alarm Group17
 Alarm Group #35
 Alarm Group Name35
 Alarm Group State Screen35
 Alarm Groups35
 Alarm Location70
 Alarm Min Level48
 Alarm on Open Loop16
 Alarm on Shorted Loop16
 Alarm Pager Setup74
 Alarm Spot Size57
 Alarm Time69
 Alarm type definitions31
 Alarm Voice Output29
 Alarm When Armed, Trouble When Disarmed on Open Loop16
 Alarm when armed, trouble when disarmed on shorted loop16
 Alarm Zone57
 Alarms38
 Alert23
 Alert Unit
 Function of8
 Alert Unit Point Type22
 Alert Units To Receivers23
 Algorithm23
All from Transponder Selected38
 Ambient51
 Analyze Alarms39
 Answer61
 Answer On Ring60
 answering machine60
 Answering Machine Override60
 Ant Map51
 Antenna51
 Area Number20

Arm Time34
 Arming State of this Alarm Group35
 Auto Advance50
 Auto Scan46
 Auto Silence Alarm In X Seconds30
 Auto synchronize time66
Autobackup to the slave database66
 Automatic by Schedule35
 Automatically Send Selected Troubles62
 Average52

B

Backup27
 Backup Screen26
 Backup/Restore to Disk Cartridge Path67
 Bad Checksum41
 Baud59
 Baud Rate62
 Beginning19
 Bring to Front on Alarm56
 Bring to Front on Trouble56
 Buddy Check55
 Buffer Overflow53
 Buffer Overflow Count54
 Bus -21
 Bus +21
 Bus fault41
 Bus Micro Revision49
 Bus X Point Y45
 Byte48

C

Cancel25, 61
 Cancel Page If Alarm Reset63
 Carrier Det58
 Cartridge67
 Cartridge Disk Drive26, 27
 Central Console9
 Function of9
 Response to Alarm11
 Central Console Response12
Character Limit62
 Classic algorithm23
 Clear EE49
 Clear Entire File27
 Clear Screen36
 Close Screen, Does Not Stop Test52
 COM58
 Comm Fail to Siren Out48
 Comm Port Index18
 Comm Port Overload42
 Communications
 failure of40
 Stress test of46
 Communications Failure38
 Computer

Master	59
Remote.....	59
Slave	59
Workstation	59
Console screen showing "Test" Icons	12
Contact Information.....	31
Control Room	57
Control Room Output to Siren.....	56
Control Room Output to Spare	56
Control Room Output to Strobe.....	56
Copy	19, 25
CR Only.....	59
CR/LF.....	59
Created.....	18
CTS Control	58
Current Check-in Status.....	36
Current Troubles.....	46
Cut	25

D

Daily Test Report.....	32
Daily Trouble Report.....	32
Database Backup and Restore	38
Database Errors	39
Database Find Level	30
Databases are not shared.....	65
dates.....	55
Day Month Format	55
Day of the Week	34
Default Master Computer	59
default password	13
Default Slave Computer.....	59
Delete.....	61
Delete Point	19
Demo Alarm	68
demo alarms.....	63
Demo Test	69
Demo Troubles	69
Device Type Map	43
Dial	61
Dialing Prefix	60
Dial-up paging modem setup	73
Direct Connect Port	59
Disable auto reconnect.....	65
Disable Idle Processing	55
Disable Open Loop.....	16
Disable Shorted Loop	16
Disabled.....	60
Disarm Time	34
Disconnect	61
Display Maintenance Alarm	55
Display Unauthorized Alarms.....	28
Done	17
Dropped.....	43

E

Edit	61
------------	----

Edit Data.....	19
Edit Schedule Times	34
Edit Schedule Times	33
Edit Subscriber's Advanced Features Screen	15
EE counters.....	49
EE Point Info	49
EE Point Stat.....	49
EE Point Trouble	49
Ellipsis (...)	34
Emergency Answer Only	59
Enable Algorithm Tweaks	55
Enable Printer	64
Enable Rec.....	52
Enable Reed Switch	16
Enable Remote Key	48
End of File	19
End Of Shift Reminder	30
Excel Test History Files.....	56
Exit	26

F

Fail To Test Letters.....	32
Failed Pager Attempts.....	53
File Menu.....	13
Filter virtual fence.....	28
First.....	35
Fixed Location and Pager Text.....	16
Fixed Location Transmitter	15
Floor	24
Floor Level	15, 23
Floppy A	27
Force Map Background Erase	55
Formfeed.....	64
Free Disk Space	69

G

Green Led	44, 50
Green Led Map.....	43
Guard Tour Exception Report	32
Guard Tour Level	30
Guard Tour Minutes	30
Guard Tour Report	32

H

Hardware Overrun	53, 54
High Speed Buddy Check.....	55
Highest.....	52
History Archive File A.....	37
History Archive File B.....	37
History Filter Output.....	60
History Filter Screen.....	37
History Screen	37
Hits	52
Hold Printer Data.....	64
Horn - Siren	44, 50
Horn - Siren Map	43

I

I'm Ok Check	44
I'm OK message	44
I'm Ok Release Control	44
ID Receiver.....	56
Idle Passes Hour	70
Idle Processing Disable	55
Idle Time	69
Ignore Communications Failure.....	18
Ignore Holidays for this Schedule.....	33
Image File Path.....	67
Importing a Subscriber Database.....	76
Incoming Communication Errors.....	52, 67
Incoming Format Errors.....	46
Incoming Retried Messages.....	46, 53, 67
Insert New.....	19, 20, 61
Installer Alarms Silent	29
Isolate From All Other Transponders For Location.....	18

J

Jam Map	51
Jamming.....	43, 51
Jamming Map	47
Jamming of Receiver	41

K

Kill Transponder.....	19
Kill Transponder button.....	19
Known Transmitters	41

L

Last	35
Last MUX Message	49
Last Remote Access Time	53
Learn address button	66
LF Only.....	59
Limit Alarms to 1 Transponder.....	29
Linear algorithm	23
Linear Depth.....	57
Load Delay	48
Load Shedding.....	46
Local Database Drive	26, 27
Local Escort Path	67
Local paging setup.....	73
Locate	15
Locate	25
Locate Test Level	30
Locate Transmitters	13
Location.....	24
Estimate of.....	11
Text to be displayed	24
Location Algorithm.....	23
Login Changes.....	39
Loop Communications.....	47
low battery.....	69
Low Battery	

Alert Unit.....	41
Transponder.....	40
Low Battery Map.....	44, 47
Low Battery Report	32
Low Depth	57
Low pull algorithm	23
Lowest	52

M

Maintenance "Alarm"	14
Maintenance Alarm.....	14, 55
Maintenance Transmitter	8, 49
Use in setup mode.....	49
Man Down Delay Timer X Seconds	30
map	61
Map.....	24
Device type, interpreting.....	43
Status, commanding and interpreting.....	42
Map File Generation.....	71
Map File Scaling.....	71
Map Number.....	15
Map Scale %	57
Map X Position.....	15
Map Y Position.....	15
Master Computer	59
Master Computer Answers.....	59
Master Computer Switch	39
Master Database Drive	26, 27
Master Database Path	66
Master's Network Address	66
Master's Network Listen Port	66
Max Man Down Messages.....	54
Max Receiver Buffer	54
Max Report Spooler Bytes.....	54
Max Spooler Bytes	54
Max Transmit Buffer	54
Max Transponders	70
Max Workstations.....	70
Maximum Alarm Messages	53
Maximum Low Battery Messages.....	54
Maximum Retry Messages.....	53
Maximum Test Strobe Messages	54
Maximum Trouble Messages.....	53
Maximum Users.....	70
Medium Depth.....	57
Medium pull algorithm	23
Midnight Report	32
Missed all Receivers	52
Misses	52
modem	55
Modem Communications.....	39
Modem Init	60, 63
Modem Port.....	58
Modem Reset	60
Modified	18
Modify Oper	18
Mon Power	58

Monitor Communications	55
Monitored Periods	42
Multiple Map Files	72
Multiplex Point	
Address, explanation of	19
Removing from service	44
Multiplex Receiver	8, 10, 12
For automatic ID# capture	56
Multiplex Receiver Parameters.....	20
MUX Bus Point Troubles	41

N

Network Comm Failure	42
Network Communications	39
Network Port	58
Network Status Screen.....	52
New Alarm Reports	32
Next	19, 35, 45, 47, 48, 49
No Buddy Check Delay	56
No CTS	58
No Password on Reentry.....	56
No Password Timeout.....	56
No Password To Exit.....	56
No Point Text If Area Text.....	29
No Receiver Icons	29
No Response	
From Multiplex Device.....	41
No Restriction	38
Not Always Top Window	56
Not Responding Map.....	43, 47
Not Testing Report	32
Number	
Area	20
Point.....	20

O

Off	45, 51
Off (disarmed)	35
On	51
On (armed).....	35
On Output Command.....	45
On Outside Tests Flash Strobe For X Seconds.....	30
Only From Transponder Selected	38
Open Loop Alarm	16
Open Loop Disable.....	16
Open Loop Trouble	16
Operator Activity Log.....	38
Operator Database	14
Operator Database Changes.....	38
Operator's Response.....	11
Option 2	29
Option 4.....	29
Option 5	29
Optional Parameter	47, 56
Optional Text.....	16
Other Time.....	70
Out of Service Map.....	47

Out Of Service Map.....	44
Outgoing Failed Messages	46
Outgoing Retried Messages	46, 53, 67
Output Device Error	41
Output includes Subscriber ID.....	29
Output includes Transmitter ID	29
Output Verification.....	36
Overload Count.....	54
Overload Level	54

P

Page to individuals.....	63
Pager	40
Send Message	63
Pager Communications	55
Pager Group.....	24, 62, 63
Pager Group.....	15
Pager ID.....	62
Pager ID.....	15
Pager Password.....	15
Pager Setup	73
Pager Text Manual.....	63
Pages Per Call.....	62
paging modem setup	73
paging service	62
password	10, 13
Password.....	9, 56, 60, 62
Password Verify.....	60
Paste	25
Personal Transmitter	7
Automatic capture of ID#	56
Disabled	12
Maintenance.....	8
Security	7
Subscriber	7
Watchman category	11
Phone Book Edit Screen	61
Phone Number	15, 62
Point.....	52
Point In Service	44
Point Number.....	20
Point Out Of Service.....	44
Point Transmitter	8
Point Troubles	39
Point Type	21, 22
Points, Reporting Alarm	38
Popup.....	40
Pop-up Trouble And Pager Delay.....	42
Pop-up Trouble Filter Screen.....	40
Power Loss	
Alert Unit.....	41
Transponder	40
Preferences Changes.....	38
Previous	19, 35, 45, 47, 48, 49
Print	32
Print	19
Print	64

Print	64
Print Report	36
Print Report Now	32
Print System Reports Screen	31
Print to File	64
Printer	37
Printer Output	39
Pulse Dial	60
Put This Receiver In Setup Mode	49

R

Radio ID	18
RAM Counters	49
RAM EE Buss Fault	49
RAM EE Mstat Batt	49
RAM Point Info	49
RAM Point Stat	49
RAM Point Trouble	49
Recall Operator In X Seconds	30
Receive Level Maps	38
Received signal strength	10
Checkbox for displaying	55
Received Transmission Map	43
Receiver	8, 10, 12
Configuration	49
Receiver 1	23
Receiver 2	23
Receiver Buffer Max	53, 68
Receiver Configuration Screen	49
Receiver floor level selection	23
Receiver Parameters	20
Receiver Point Type	22
Receiver Sensitivity Adjust	24
Receiver Test Screen	51
Receiver's Response	10
Receivers Not Heard From Report	32
Red Led - Strobe	51
Reed Switch	16
Refresh Data	47, 53, 54, 68
remote access	61
Remote Computer	59
remote connection	61
Remote Connection Screen	60
Remote Key Activation	41
Remote Key Tamper	41
Remote Port Setup Screen	58
Remote Setup Screen	59
Remote System Control	60
Remove	34
Report	
End of shift reminder for	30
Trouble, filtering	39
Report Database Changes	38
Reports Database	14
Require Alarm Report	29
Requires Check-in	17
Reset Max	70
Reset Point	51
Reset Status	53, 54, 68
Reset Transponder	44
Reset Transponder Troubles	47
Restarted	43
Restore	27
Restore save old database message box	28
Restore Screen	27
Restore to Disk Cartridge Path	67
Restore warning message box	28
Revision	51
RF Micro Version	51
RF Point Troubles	38
Run Buddy Check	55
Run Silent	47
Run Test	52

S

SA%	24
Save	25
Save Changes Screen	25
Save EE	49
Scaling	67
Schedules	33
Security Alarms Silent	29
security pager	63
Security Pager Setup	74
Security Preferences	28
Unauthorized Transmitters	11
Security Preferences Screen	28
Security Transmitter	7
Select	64
Select Point Screen	21
Send All Other Alarms	63
Send Change	48
Send Installer Demo Alarms	63
Send Page a Second Time, 2 Minute Delay	63
Send Pager Message Screen	63
Send Security	63
Send Service	63
Send to Group	63
Send to Individual	63
Sensitivity Adjust	24
Serial Number	70
service pager	62
Service Pager Setup	74
Setup menu	37
Shift Reminder	30
Shorted Loop Alarm	16
Shorted Loop Disable	16
Shorted Loop Trouble	16
Show all error pop-ups	65
Show Areas	20, 22
Show connection pop-ups	65
Show History	36
Show Maintenance Levels	55
Show Map	36

Transponder Outputs	44
Transponder Parameter Change Screen	47
Transponder Scanning	10
Transponder Startup	41
Transponder Troubles.....	39
Trouble	56
Current device status.....	46
Emergency contact text box for	31
Trouble on Open Loop	16
Trouble on Shorted Loop.....	16
Trouble Response Text.....	20
Trouble Tamper Text.....	20
Trouble Type Text.....	20
Troubles.....	62
Turn On Alarm Strobes	28
Turn On Outside Sounders	28

U

Uninstalling the Security Escort program	13
Unknown Transmitters.....	41
Unlimited Retries.....	45
Uses Proxim Radio	48
Utilities Menu.....	26

V

Verbose Point Reports	48
Verify Password.....	62
Video Switcher	24
Video Switcher Control	60
Video Switcher Restore	60
View Alarm Groups.....	34
View Alarm Groups.....	33
virtual fence	28
virtual fence alarm	16
Virtual Fence Alarm	25
Virtual Fence Area.....	25
virtual receiver	23
Virtual Receiver Point Type	22

W

Weekly Maintenance Test Report.....	32
Weekly Security Test Report	32
Weekly Subscriber Test Report	32
Weekly Watchman Test Report	32
Wondering Alarm	25
Workstation Computer.....	59

Bosch Security Systems
130 Perinton Parkway
Fairport, NY 14450-9199
Customer Service: (800) 289-0096
Technical Support: (888) 886-6189

© 2003 Bosch Security Systems
38947D

BOSCH

Free Manuals Download Website

<http://myh66.com>

<http://usermanuals.us>

<http://www.somanuals.com>

<http://www.4manuals.cc>

<http://www.manual-lib.com>

<http://www.404manual.com>

<http://www.luxmanual.com>

<http://aubethermostatmanual.com>

Golf course search by state

<http://golfingnear.com>

Email search by domain

<http://emailbydomain.com>

Auto manuals search

<http://auto.somanuals.com>

TV manuals search

<http://tv.somanuals.com>