Security Escort

SE2000 Series

en Hardware Installation Manual

Table of contents

1	**About this manual**	**5**
1.1	Agencies	5
1.2	General information	5
1.3	Safety symbols and their meanings	5
1.4	Conflicts with other documents	6
1.5	Trademarks	6
2	**System overview**	**7**
2.1	System components description	7
2.2	Compatible parts	8
2.3	System components and specifications	8
2.3.1	Central Console	8
2.3.2	EA500 transponder	10
2.3.3	EA102 receiver	10
2.3.4	EA120 alert unit	11
2.3.5	Moxa interface adapter	11
2.3.6	Lantronix interface adapter	11
2.3.7	SE485 interface adapter	12
2.4	Transmitters	12
2.4.1	Personal Escort transmitters	12
2.4.2	SE2 personal transmitter	13
2.4.3	SE3 subscriber transmitter family	14
2.4.4	SE3401 point tracking transmitter	14
2.5	Cables	14
2.5.1	Master to slave	15
2.5.2	Moxa to transponder (not supplied)	15
2.5.3	Lantronix to transponder (not supplied)	15
2.5.4	Computer to SE485 (not supplied)	15
2.6	Batteries	16
2.6.1	E28629B, Special 3 Ah	16
2.7	Enclosures	16
2.7.1	AE1, Small Indoor Enclosure	16
2.7.2	AE3, Large Indoor Enclosure	16
2.7.3	AE100 Indoor Enclosure	17
2.7.4	AE101 Outdoor Enclosure	17
2.8	Miscellaneous	17
2.8.1	Siren Strobe	17
3	**Equipment estimation**	**18**
3.1	Location accuracy	18
3.2	Pre-bid equipment estimation	19
3.2.1	Initial equipment estimate	19
3.3	Pre-construction coverage verification survey	21
3.3.1	Verify each potential receiver location	21
3.3.2	Indoor receiver installation	22
3.3.3	Outdoor receiver installation	23
3.4	Post construction setup	24
3.4.1	Testing the location accuracy of an installation	24
3.4.2	Improving the location accuracy of an installation	26
4	**Installation instructions**	**29**

4.1	Overview of installation process	29
4.2	Run system wiring	29
4.2.1	General guidelines	29
4.2.2	Observe established standards	30
4.2.3	Transponder wiring notes	35
4.2.4	Receiver wiring notes	35
4.2.5	Alert unit wiring notes	35
4.2.6	Moxa interface wiring notes	35
4.2.7	Lantronix interface wiring notes	38
4.2.8	SE485 interface wiring notes	41
4.3	Mounting the enclosures	42
4.3.1	AE1 small indoor enclosure	42
4.3.2	AE3 large indoor enclosure	42
4.3.3	AE100 indoor enclosure	43
4.3.4	AE101 outdoor enclosure	44
4.4	Mounting and setting up components	45
4.4.1	EA102 receiver installation	45
4.4.2	EA500 transponder installation	45
4.4.3	EA120 alert unit installation	47
4.4.4	ProxLink setup	49
5	**System power-up and debug**	**51**
5.1	Initial system configuration	51
5.2	Powering up the system for the first time	51
6	**Testing and troubleshooting**	**55**
6.1	Built-in troubleshooting aids	55
6.1.1	EA102 receiver	55
6.1.2	EA500 transponder	56
6.2	Troubleshooting reference	59
6.3	Software Troubleshooting	68
6.3.1	“CAN'T OPEN THE OPERATOR.EDB FILE” error	69
6.3.2	Network connection fails	69
6.3.3	“THE MASTER COMPUTER MUST BE ON-LINE TO RETURN THE SYSTEM TO OPERATIONAL STATUS” message	70
7	**Appendix: Information sheet and files required**	**71**
7.1	Transponder information sheet	71
7.2	Files required for Security Escort	73
	Index	**76**

1 About this manual

1.1 Agencies

Consult the documentation accompanying each component for specific listings.

1.2 General information

The purpose of this manual is to identify the components of the Security Escort system, provide installation instructions for those components as well as the system as a whole provide testing procedures for the system and its components, and provide a troubleshooting guide. The sections of this manual are as follows:

- *System overview, page 7*: This section provides a reference for estimating and ordering components for a Security Escort installation. Attention is given to relevant specifications of individual components to assist an installer in providing accurate bid estimation.
- *Equipment estimation, page 18*: This section serves as a guide to estimating the equipment needed for a bid, the location accuracy to expect, and how to mount the receivers to achieve that accuracy.
- *Installation instructions, page 29*: This section provides an overview and quick reference for the overall installation of a Security Escort System. Consult the *Installation Instructions* that accompany each individual Security Escort component for specific installation and set-up instructions for that component.
- *System power-up and debug, page 51*: This section includes information on making the system “live” after all components are installed and wired.
- *Testing and troubleshooting , page 55*: This section provides procedures for ensuring that the system is “live” and functional. Also, a troubleshooting guide is provided in the event that some components do not respond to the system.
- *Appendix: Information sheet and files required, page 71*: The *Appendix* provides additional information and forms that may be useful before and during installation.

If you encounter any problems or questions that are not covered in this manual, contact Bosch Security Systems Technical Support at the phone number listed on the back page of this manual.

1.3 Safety symbols and their meanings

Throughout this document, the following symbols are used to alert the reader to safety issues when installing or operating the system:

Notice!
This symbol alerts the reader to possible equipment damage if procedures are not followed correctly. For example, “Do not connect the positive wire to the negative terminal.”

Caution!
This symbol informs the reader of possible bodily injury if procedures are not followed exactly. The text accompanying this symbol tells the reader what he should or should not do. For example, “Ensure that you are properly grounded before opening the unit.”

1.4 Conflicts with other documents

In addition to this manual, the installer is directed to review installation instructions that accompany individual components, and release notes. In the event of a discrepancy between the information provided in this document, and the information provided in a document accompanying a specific component (or release notes), the information contained in the installation instructions or release notes shall prevail.

1.5 Trademarks

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

2 System overview

2.1 System components description

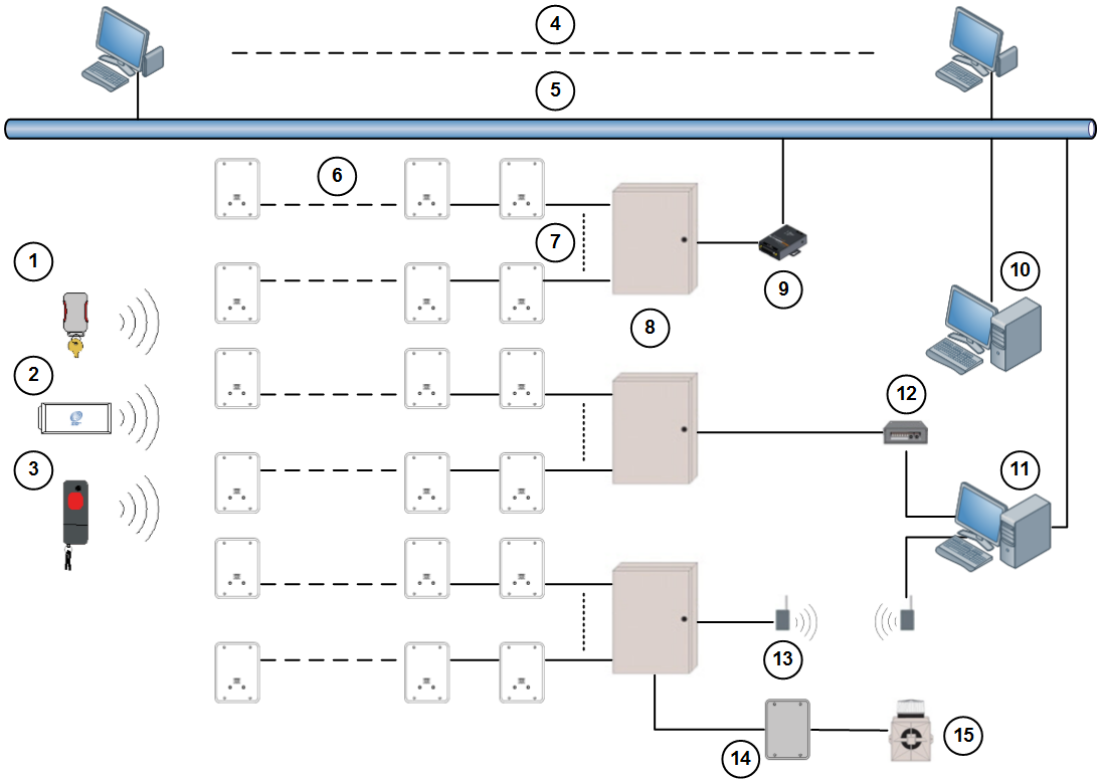


Figure 2.1: System Block Diagram

1	Subscriber transmitter	9	Serial to Ethernet interface
2	Point tracking transmitter	10	Slave workstation
3	Personnel transmitter	11	Master workstation
4	Up to 8 workstation	12	SE485 interface
5	LAN	13	Spread spectrum wireless links
6	Up to 8 receivers	14	Alert unit
7	Up to 8 bus	15	Strobe
8	Transponder		

The **transmitter** is a miniature, hand-held radio transmitter used to transmit either a distress or a test signal. The **receivers** are located throughout the 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 (plus an optional backup and up to 8 optional workstations) which receives alarm and trouble signals

from the transponders, analyzes the signals, activates strobes and sirens on the alert units, and produces a display for the Security dispatcher. Each of these system elements is described more fully in the sections that follow.

2.2 Compatible parts

The following table indicates the parts available for inclusion in a Security Escort system. Contact Bosch Security Systems Customer Service for up-to-date model numbers.

Part Name	Description
Electronics, Components	
EA500	Electronics for eight-bus transponder
EA102	Electronics for indoor or outdoor receiver
EA120	Electronics for indoor and outdoor alert unit
SE485	Interface between transponder and Central Console
SE2 transmitters	Man-down, lanyard, supervisory, and duress transmitter
SE3401	Point tracking transmitter
SE88	Personal watch/Pendant transmitter
Enclosures and Housings	
AE3	Large enclosure, 51.5 cm x 37.5 cm (20.25 in x 14.75 in)
AE1	Small enclosure, 36.8 cm x 31.8 cm (14.5 in x 12.5 in]
AE100	Indoor receiver enclosure
AE101	Outdoor receiver enclosure
Software	
SE2005	System software for up to 500 users
SE2010	System software for up to 1,000 users
SE2050	System software for up to 5,000 users

2.3 System components and specifications

2.3.1 Central Console

Description

The Central Console consists of one or two computers (and up to 8 additional workstations) running the Security Escort software within the Microsoft Windows environment. One computer serves as the master controller for the entire Security Escort system and the second slave computer serves as a back-up. The slave computer can be used for administrative functions such as adding subscribers or performing routine system tests without interfering with the operation of the main computer. The workstations can perform all normal Security Escort functions with the exception of communicating with the transponders.

Software overview

The Central Console contains all of the operating software and all of the databases required by the Security Escort system. 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. The system software also continually monitors the status of each transponder to ensure it is functioning correctly.

Versions

There are several versions of the software available. The number of users the system will support defines each version. The following table lists the available models and the number of supported users:

Model	User Base
SE2005	500
SE2010	1,000
SE2050	5,000

Notice!

For systems supporting more than 5,000 users contact Bosch Security Systems Sales.

Minimum system requirements

As a minimum, each computer in the Central Console should be equipped with the following features and components:

- **Processor:** 1 GHz or faster.
- **Operating system:** Microsoft Windows XP®, Windows 7® 32/64-bit, Windows 8/8.1® 32/64-bit, Windows 10® 32/64-bit
- **RAM:** Minimum 2 GB, due to .NET requirement
- **Hard disk space:** 1 GB of hard disk space should be available to allow collection of historical data
- **Backup:** External backup drive for backup and history storage.
- **Video:** VGA (640 x 480) at 256 colors minimum, 800 x 600 High color (16 bits) recommended, 1024 x 768 High color supported. True color (24 bits) is also supported. If displaying subscriber images, High color (16 bits) or True color (24 bits) should be used.
- **Modem:** Optional V.32bis (14.4), V.34 (33.8), or V.90 (56.6) modem for remote access and pager dial-out. If modem is external an additional serial port is required.
- **Sound:** Any Windows compatible sound system. One set of computer speakers per computer.
- **Printer:** Parallel or network printers.
- **Additional serial ports (if needed):** Any multi-port board fully supported by Windows. A four-port ISA serial port card made by Digiboard, model AccelePort Xe, part number 76000035. Required four-port cable for DB25, part number 76000008. Digiboard also makes eight- and sixteen-port solutions. They may be contacted at www.digiboard.com.

Databases

- **Alarm reports:** Each alarm is saved as a record containing subscriber data, time and date of alarm, acknowledgment and silence times, responding officer, problem description, and action taken. The alarm map can be reproduced and the location text is displayed.
- **History:** A complete chronological history of all system actions, tests, and alarms is recorded.

- **Operators:** File of those authorized to use the Security Escort system.
- **Subscriber:** Complete record of all subscriber data and current status, low battery, and last test date and time.
- **Transponders:** System configuration containing all installed equipment and system interrelationships.

Other Specifications

- **Temperature range**: 0 ºC to +40 ºC (+32 ºF to +105 ºF)
- **Primary power:** 120 V AC 900 W (two computers, two monitors and one printer).
- **Backup power:** 1200 V A UPS per computer will provide 45 minutes to one hour backup. System should also be backed up by an emergency generator for extended blackouts (can be shared with other emergency equipment).
- **Pager:** Pager support is included and selected troubles can be automatically sent to a service pager.

2.3.2 EA500 transponder

Description

The transponder is a device controller for up to 64 devices; and any combination of receivers and alert units. The devices are connected to the transponder by means of four-wire buses; two for power and two for data. There are eight buses and each bus is capable of supporting up to eight devices. The Security Escort system supports up to 255 transponders.

Specifications

- **Compatible Enclosures:**
  - Small indoor: AE1
  - Large indoor: AE3 (recommended)
- **Temperature range:** -40 °C to +65 °C (-40 °F to +149 °F)
- **Power Source:** 18 V AC, 50 V A (can use TR1850, 110 V AC to 18 V AC transformer)
- **Battery backup:** 12 V DC lead acid battery
- **Power output:** 9 V DC output for SE485 or for ProxLink Radio Module power
- **Driver outputs:**
  - Strobe: 500 mA solid state sink, terminal switches to ground in an alarm condition.
  - Siren: 500 mA solid state sink, terminal switches to ground in an alarm condition.
- **Multiplex buses:** eight multiplex driver buses for power and communication to receivers or alert units
- **Communication interface to Central Console:** selectable TCP/IP, SE485 or RS-232
- **Keyswitch input:** Optional 47k EOL resistor, supervised loop

2.3.3 EA102 receiver

Description

The EA102 receivers are located throughout the grounds and building interiors. Each receiver contains a radio receiver to detect the transmissions from transmitters. Multiple receivers detect the same transmission and send the signal information to the transponder so the system can identify the transmitting device, transmitting information, and location. The receiver also reports housing tampering and radio jamming to the transponder.
Indoor receivers are typically mounted on inside walls and have one red and one green LED. The green LED is used to indicate a successful Test of a personal transmitter. The red LED is illuminated during alarms. Each receiver contains a piezoelectric horn that can be activated if the receiver detected an alarm transmission.

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 LEDs. Outdoors, the strobe lights on the alert units should be used to acknowledge successful test and alarm.

Specifications

- **Enclosure:**
  - Indoor: AE100 indoor enclosure
  - Outdoor: AE101 outdoor enclosure
- **Temperature range:** -40 °C to +65 °C (-40 °F to +149 °F)
- **Power source:** 12 V DC, 25 mA typical, 55 mA with horn sounding, supplied from the transponder MUX bus
- **Antenna type:** Diversity antennas protected within enclosures

2.3.4 EA120 alert unit

Description

This is a control module that communicates with the transponder on the MUX bus. The alert unit can be used to activate strobe and siren units or optional other switched devices. The alert unit also reports tampering, AC power loss, and backup battery level to the transponder.

Specifications

- **Enclosures:**
  - Indoor: AE1 small indoor metal
  - Outdoor: AE101 outdoor fiber
- **Temperature range:** -40 °C to +65 °C (-40 °F to +149 °F)
- **Power source:** 18 V AC, 50 VA (can use TR1850, 110 V AC to 18 V AC transformer)
- **Battery backup:** 12 V DC lead acid battery
- **Driver outputs:**
  - Power: 1 A maximum, intended as the supply source for strobe and siren
  - Strobe: 500 mA solid state sink, terminal switches to ground in an alarm condition
  - Siren: 500 mA solid state sink, terminal switches to ground in an alarm condition

2.3.5 Moxa interface adapter

Description

The Moxa device is an interface between the RS-232 signal bus of the Security Escort transponder and the Ethernet port of the Security Escort Central Console. The Moxa device allows transponders to use TCP/IP protocol to communicate with the Central Console.

Specifications

- **Dimensions:** 5.2 cm x 8.0 cm x 2.2 cm (2.05 in x 3.15 in x 0.89 in)
- **Power Source:** 12 – 48 V DC
- **Temperature range:** 0 °C to +55 °C (+32 °F to +131 °F)
- **Ethernet interface:** 10/100 Base-T

2.3.6 Lantronix interface adapter

Description

The Lantronix device is an interface between the RS-232 signal bus of the Security Escort transponder and the Ethernet port of the Security Escort Central Console. The Lantronix device allows transponders to use TCP/IP protocol to communicate with the Central Console.

Specifications

- **Dimensions:** 9.5 cm x 7.2 cm x 2.3 cm (3.7 in x 2.8 in x 0.9 in)
- **Power Source:** 9 – 30 V DC
- **Temperature range:** 0 °C to +60 °C (+32 °F to +140 °F)
- **Ethernet interface:** 10/100 Base-T

2.3.7 SE485 interface adapter

Description

The SE485 is an interface between the pseudo RS-485 signal bus of the Security Escort transponder and the serial bus (RS-232) of the Security Escort Central Console. The SE485 allows multiple transponders to interface into a single RS-232 port.

Due to changes made for transient protection, transformer isolation, and link busy detection, these signals are not compatible with third party RS-485 interfaces.

Specifications

- **Dimensions:** 13.5 cm x 8.5 cm x 30 cm (5.375 in x 3.3125 in x 1.1875 in)
- **Power Source:** 9 V DC, 200 mA. An included 120 V AC adapter to 9 V DC or from the transponder 9 V DC terminals.
- **Temperature range:** 0 °C to +65 °C (+32 °F to +149 °F)

2.4 Transmitters

2.4.1 Personal Escort transmitters

Notice!
Not all features are available on all transmitters.

- **Unique ID code:** All personal Escort transmitters contain a unique identification that can be entered into the Central Console system database. This allows the system to only respond to appropriate users and ignore unauthorized devices. It also allows unique identification of owner in database.
- **Local piezo sounder:** All personal Escort transmitters contain an internal piezo sounder device. The piezo is sounded during most types of transmissions to indicate to the user that the alarm or test event was activated.
- **Duress alarm (manual alarm):** All personal Escort transmitters allow an alarm condition to be transmitted by the user manually activating the alarm buttons**.**
- **Transmitter test:** All personal Escort transmitters allow the user to activate the transmitter to perform a system test. This tests that the system acknowledges the transmitter, the receivers in the area function, the transponder communication functions, and the particular transmitter ID are in the Central Console database.
- **Man-down:** Some transmitters contain an internal “tilt” switch that monitors and transmits an alarm if the transmitter is not in an upright position.
- **Supervision:** Some transmitters send periodic transmissions, allowing the system to monitor activity of the transmitter and report failing transmitters or missing transmitters.

Notice!
Supervision transmissions do not activate the local piezo sounder.

- **Lanyard:** Some transmitters contain a “pull switch” that transmits an alarm if the lanyard is pulled from the transmitter unit.
- **Auto tracking:** When an alarm is transmitted, the transmitter continues to transmit periodically for 15-min. following the alarm. This allows the system to track a moving transmitter that is activated.
- **Silent manual alarm (“security”):** This feature is available on security transmitters. When the duress alarm (manual alarm) is activated by the user, there is no local sounder turned on. This allows users to transmit the alarm silently.
- **Maintenance transmitter:** Used to validate the system functions. By performing a test, the receiver indicates receptions by lighting the green LED. Transmitting an alarm lights up the red LED. The maintenance transmitters do not activate a real system alarm, the system uses the information for diagnostic and test purposes only. There is no auto tracking on the maintenance transmitters.
- **Low battery indication:** The battery status is sent with each transmission, the system tracks and reports low battery devices.

2.4.2 SE2 personal transmitter

Description

There are several versions of the SE2, and these versions along with their respective features are shown in the table below.

Feature	Model				
	SE2S	SE2U	SE2M	SE2S-SN	SE2U-SN
Manual duress alarm	✓	✓	✓	✓	✓
Manual test	✓	✓	✓	✓	✓
Man-down	✓	✓	✓	✓	✓
Supervision	✓	✓		✓	✓
Lanyard snatch				✓	✓
Auto tracking	✓	✓		✓	✓
Silent manual alarm	✓			✓	
Low battery indication	✓	✓	✓	✓	✓

Tab. 2.1: SE2 Personal Transmitter Features

Notice!
Due to communications limitations between the transponder and receivers, a maximum of 200 supervised SE2 transmitters can be handled in a Security Escort system.

Specifications

- **Battery:** User replaceable 3 V lithium
- **Temperature range:** -30 ºC to +65 ºC (-22 ºF to +150 ºF)

2.4.3 SE3 subscriber transmitter family

Description

The SE3 subscriber transmitter is a personal duress transmitter that contains the manual duress alarm, manual test, and auto tracking features.

Feature	Model	
	SE3U	SE3S
Manual duress alarm	✓	✓
Manual test	✓	✓
Auto tracking	✓	✓
Silent manual alarm		✓
Low battery indications	✓	✓

Tab. 2.2: SE3 Subscriber Transmitter Features

Specifications

- Battery: Two user replaceable 3 V DC lithium coin cells (CR2025 size)
- Temperature range: -30 ºC to +65 ºC (-22 ºF to +150 ºF)

2.4.4 SE3401 point tracking transmitter

Description

The SE3401 point transmitter is a magnetic and dry contact wireless transmitter used for monitoring assets.

The unit is equipped with an internal reed contact for use with an external magnet assembly (included), a cover tamper switch and RF supervision. The SE3401 also can accept a supervised dry contact input from an external device.

Specifications

- **Dimensions:**
  - Transmitter w/o mounting plate: 35 mm x 76.5 mm x 19 mm (1.5 in x 3.25 in x .75 in)
  - Mounting plate: 35 mm x 76.5 mm x 3.2 mm (1.5 in x 3.25 in x .125 in)
- **Operating temperature:** -20 °C to +65 °C (-4 °F to +150 °F)
- **Operating voltage:** Supplied by a 3 V DC lithium battery.
- **Battery life:** Up to five years under normal usage with the recommended battery types. Higher usage decreases battery life.
- **Recommended battery types:** Duracell DL123A, Energizer EL123AP, or Panasonic CR123A.
- **Compatible receivers:** EA102A-304

2.5 Cables

2.5.1 Master to slave

Notice!
This cable is not supplied by Bosch Security Systems.

Description
Null modem cable connecting the two computers running the Central Console software.

Specifications
- **Maximum Length:** 15 m (50 ft)
- **Connectors:** To be compatible with your PC's requirements.

2.5.2 Moxa to transponder (not supplied)

Notice!
This cable is not supplied by Bosch Security Systems.

Description
This cable connects the transponder to the serial port of the Moxa interface.

Specifications
- **Maximum length:** 15 m (50 ft)
- **Connectors:** The Moxa uses a DB9 pin female connector while the transponder uses a DB9 pin male connector. The wiring is a straight-through serial cable.

2.5.3 Lantronix to transponder (not supplied)

Notice!
This cable is not supplied by Bosch Security Systems. The default cable supplied with the Lantronix interface cannot be used as modifications are required.

Description
This cable connects the transponder to the serial port of the Lantronix interface.

Specifications
- **Maximum length:** 15 m (50 ft)
- **Connectors:** The Lantronix uses a DB25 pin male connector while the transponder uses a DB9 pin male connector. Special wiring is required.

2.5.4 Computer to SE485 (not supplied)

Notice!
This cable is not supplied by Bosch Security Systems.

Description
This cable connects the SE485 Interface to the serial port of the Security Escort Central Console.

Specifications
- **Maximum length:** 15 m (50 ft)
- **Connectors:** The SE485 uses a DB25 pin male connector, the other end depends on the computer serial port connector. The wiring is a straight-through serial cable.

2.6 Batteries

Bosch Security Systems recommends that you supply your own 12 V lead-acid batteries for system component back-up time as needed for your installation. However, some of the standard battery sizes can be supported. See table below for the required amp hours of the batteries for your installation.

Number of Hours	Amp hours (Ah) Required per Number of Receivers			
	8	16	32	64
4	2.3	3.5	5.7	10.2
8	4.6	7.0	11.4	20.4
12	7.0	10.3	17.0	30.6
24	14	20.6	34.0	---

Tab. 2.3: Battery Amp Hours

2.6.1 E28629B, Special 3 Ah

Description
Special size used especially for the outdoor alert unit.

Specifications
- **Dimensions:** 6.3 cm x 13.3 cm x 6.3 cm (2.5 in. x 5.25 in. x 2.5 in.)
- **Amp-hours:** 3 Ah
- **Voltage:** 12 VDC

2.7 Enclosures

2.7.1 AE1, Small Indoor Enclosure

Description
The AE1 Enclosure is suitable only for indoor installation. A mounting kit for the electronic components is included.

Specifications
- **Dimensions:** 36.8 cm x 31.8 cm x 8.6 cm (14.5 in. x 12.5 in. x 3.375 in.)

2.7.2 AE3, Large Indoor Enclosure

Description
The AE3 is suitable only for indoor installation. A mounting kit for the electronic components is included.

Specifications
- **Dimensions:** 52.7 cm x 38 cm x 10.8 cm (20.75 in. x 15 in. x 4.25 in.)

2.7.3 AE100 Indoor Enclosure

Description

The AE100 Indoor Enclosure houses the receiver. It is suitable only for indoor installation.
Mounting screws: Security design, require E28666B security hex driver

Specifications

– **Dimensions:** 22.9 cm x 17.8 cm x 14.4 cm (9 in. x 7 in. x 1.75 in.)

2.7.4 AE101 Outdoor Enclosure

Description

This enclosure houses the receiver or alert unit. It is suitable for outdoor installation. The receiver's LEDs and sounder cannot be used in this enclosure. A mounting kit for the electronic components is included.

Specifications

– **Dimensions:** 27.2 cm x 18.2 cm x 9.2 cm (10.7 in. x 7.2 in. x 3.6 in.)

2.8 Miscellaneous

2.8.1 Siren Strobe

The armored siren with strobe can be purchased through third-party vendors. Bosch Security Systems recommends Amseco Armored Siren with Strobe (model number SSX-51S).

3 Equipment estimation

A Security Escort system installation consists of three major steps:

1. the pre-bid equipment estimation,
2. the pre-construction coverage verification survey, and
3. the post construction setup.

The Security Escort receivers work effectively in a wide variety of installations and can be placed with confidence provided these installation requirements are met. Therefore, at the pre-bid stage, it is acceptable to estimate the required equipment. To ensure proper coverage after proposal acceptance, potential receiver locations can be verified using a standard receiver in test mode or the portable test receiver before construction begins.

3.1 Location accuracy

The Security Escort system provides quick response to a duress call. Its intent is to dispatch a responding individual to an area without additional delay to their response to that duress call.

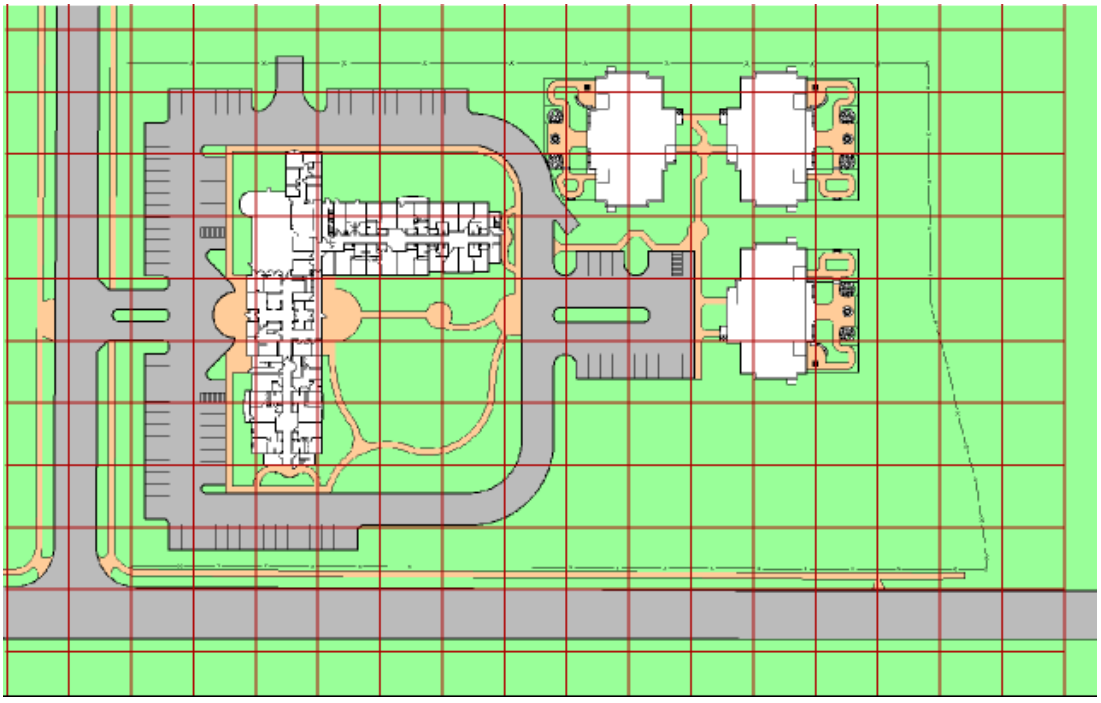


Figure 3.1: System Block Diagram

The Security Escort system uses radio frequency (RF) for alarm transmissions. This is significant because it prevents normal construction from blocking the signal and helps to eliminate dead spots where the alarm could not be heard. The fact that RF energy passes through normal construction prevents Security Escort from locating an alarm with 100% certainty to a specific side of a wall. Alarms originating at or near building walls will typically be indicated within 7.5 m (25 ft) of the actual location. However, there may be times when the computed location may appear to be on the other side of the wall.
The Security Escort system was designed to provide a computed alarm location typically within 7.5 m (25 ft) of the actual location when indoors, and a computed alarm location typically within 15 m (50 ft) of the actual location outdoors. Any deviation from the following installation guidelines will degrade the computed location accuracy. Therefore, to achieve accuracy, the following installation guidelines must be adhered to.

3.2 Pre-bid equipment estimation

The pre-bid equipment estimation is performed prior to bidding the installation. At this point, it must be determined what type of coverage is desired, and where the coverage will be required. For example, the amount of equipment required for a full-coverage (indoor and outdoor) system in a multi-building application is greater than an installation that requires outdoor only coverage. The customer should be consulted, and the areas of most concern should be given special consideration.

3.2.1 Initial equipment estimate

Number of indoor receivers

To estimate the number of indoor receivers, first read *Indoor receiver installation, page 22*. Assume the receivers are placed on a grid with a maximum spacing of 25 m (80 ft) between receivers for standard construction. In multi-floor applications the receivers on each floor must be placed directly above the receivers on the floor below (this is required for proper floor-to-floor location).

For example, to determine the number of receivers required to protect a building of standard construction of 60 m x 30 m (200 ft x 100 ft) and four floors:

1. To determine the number of receivers in each direction, divide each dimension of the building by 25 m (80 ft), drop the remainder, and add 1. For example:
   - 60 m/25 m = 2.4, becomes 2, add 1 = 3
     (200 ft/80 ft = 2.5, becomes 2, add 1 = 3)
   - 30 m/25 m =1.2, becomes 1, add 1 = 2
     (100 ft/80 ft =1.25, becomes 1, add 1 = 2)
2. To determine the number of receivers required per floor, multiply the number of receivers in one direction by the number of receivers in the other direction.
   (3 x 2 = **6**) 6 receivers per floor.
3. To determine the total number of receivers, multiply the number of receivers per floor by the number of floors.
   (6 x 4 = **24**) 24 receivers for the building.

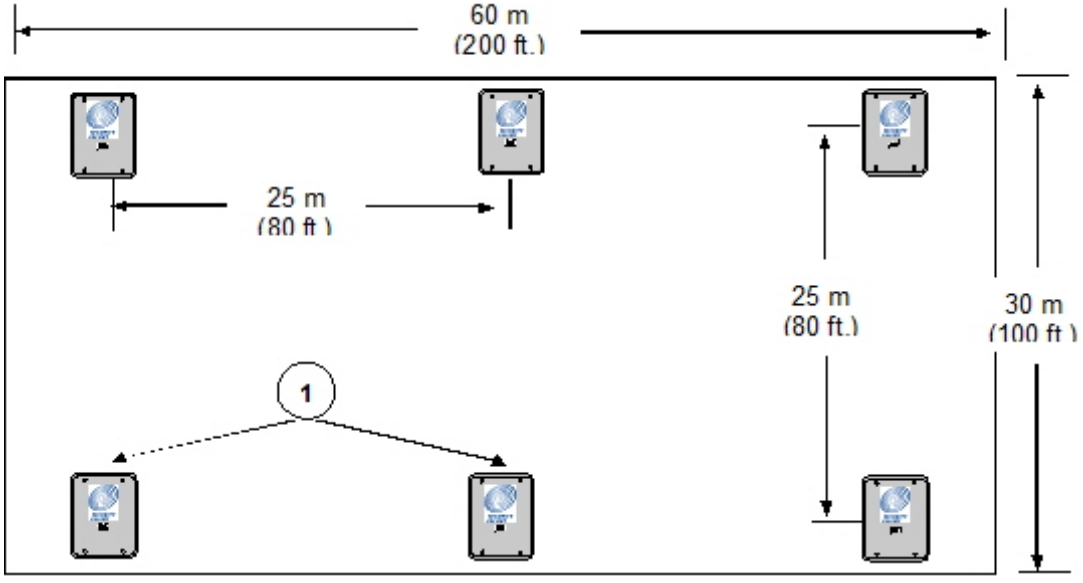
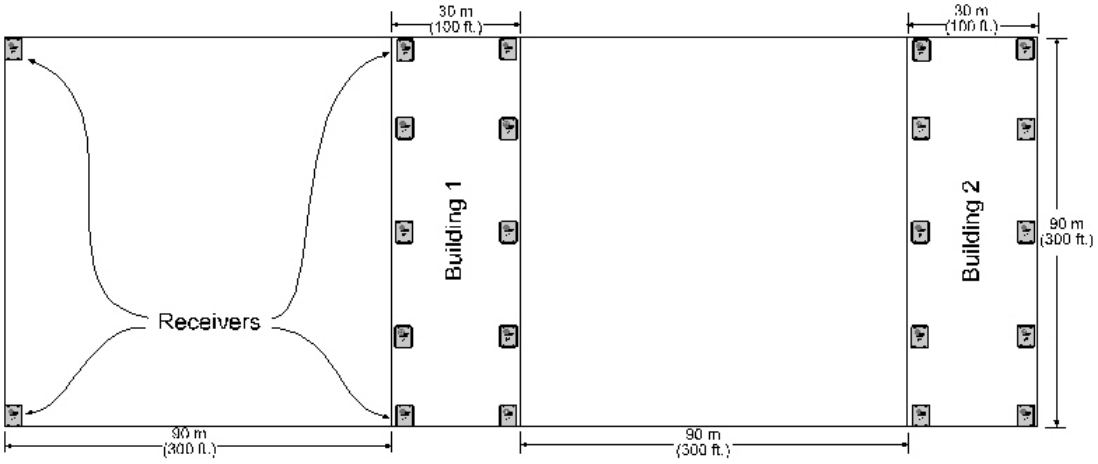


Figure 3.2: Determining the Number of Indoor Receivers Required

1	Receivers (6)		

Each floor would require 6 receivers, resulting in a total of 24 receivers to protect this building.
For the best location accuracy, consistent receiver spacing is important. Do not place receivers significantly closer in one section of a building than another section.

Number of outdoor receivers



To estimate the number of receivers, first read *Outdoor receiver installation, page 23*. Assume a maximum receiver spacing of 90 m (300 ft) between receivers, in both directions, for receivers that are not within 30 m (100 ft) of a building with inside coverage. Receivers within 30 m (100 ft) of a building should be spaced the same as receivers in the building (spacing the outside receivers at a somewhat larger spacing is acceptable in most cases).
An outside area directly between two buildings with inside protection will need no additional receivers if the buildings are 90 m (300 ft) or less apart. If the buildings are more than 90 m (300 ft) apart the outside receivers should be evenly spaced between the buildings. Make sure the standard 90 m (300 ft) spacing is not exceeded. For spacing outside adjacent to a covered building, start the 90 m (300 ft) spacing at the building wall.

Allowance for special coverage requirements
For purposes of the bid, the number of receivers estimated above should be raised by 5% to allow for special coverage considerations and RF problem areas.

Number of transponders
Assume one transponder per building for indoor installations. If wiring can be run from other buildings or from outdoor receivers, they may be connected to one transponder. Never exceed the total number of 64 devices (receivers and alert units) per transponder. All outside wiring must be under ground, or in metal conduit.

Number of receivers and alert units per bus
For transponders, each bus can handle 8 receivers and alert units. However, it is a good idea to leave some addresses available on each bus to allow for future expansion. For systems with a high number of supervised transmitters, see *Transponder wiring notes, page 35*.

Bus wire
The multiplex bus for transponder should be wired with 4 conductor 18 gauge (1.2 mm) wire. The wire should not be paired or shielded. In the United States this is the same as fire system wire, except it should not be red.

Number of alert units
The number of alert units will be determined by each system's requirements. In general, enough alert units should be installed to be heard and seen from all outdoor locations of protection. Remember that even in a silent system, alert units can be used outside to provide test feedback. Horn/strobe units should be mounted in predictable locations to make them easy to identify by subscribers. Alert units are not required indoors because the indoor receiver provides alarm and test feedback. Each transponder will drive one siren and one strobe if they are less than 15 m (50 ft) from the transponder.
It is a good idea for each protected parking lot to have a siren/strobe near it.

3.3 Pre-construction coverage verification survey

The pre-construction coverage verification survey is performed after the bid is accepted and before construction begins. It is done to determine the location of each receiver. Each receiver location should be checked using a standard receiver in the test mode.

3.3.1 Verify each potential receiver location

Using a receiver in "receiver spacing" mode
"Receiver spacing" mode is enabled with jumper P5 in place (jumper P4 removed) on a receiver (see the *EA102 Receiver Installation Instructions*).
This mode is exactly the same as the "test" mode, except that only transmissions with an adequate receive margin are sounded. This indicates the maximum acceptable spacing of receivers. Use the following procedure to test the spacing of receivers:

1. Mount the first receiver.
2. Put jumpers P1, P2, P3, and P5 in place, and remove all other jumpers. Power the receiver from a or 12 VDC source.
3. Take the second receiver and a transmitter a distance away from the first receiver.
4. Activate the transmitter.
5. If receiver 1 sounds the test beep, receiver 2 is within range. Repeat this test until receiver 1 no longer sounds the test beeps. Move back to the last location where receiver 1 received the test beeps. This location marks the maximum spacing between receivers. The distance between receivers should not exceed 25 m (80 ft) indoors and 90 m (300 ft) outdoors. Mount receiver 2 at this location or closer to receiver 1.

Notice!
Do not use the "test" mode (jumper P4) to determine receiver spacing.

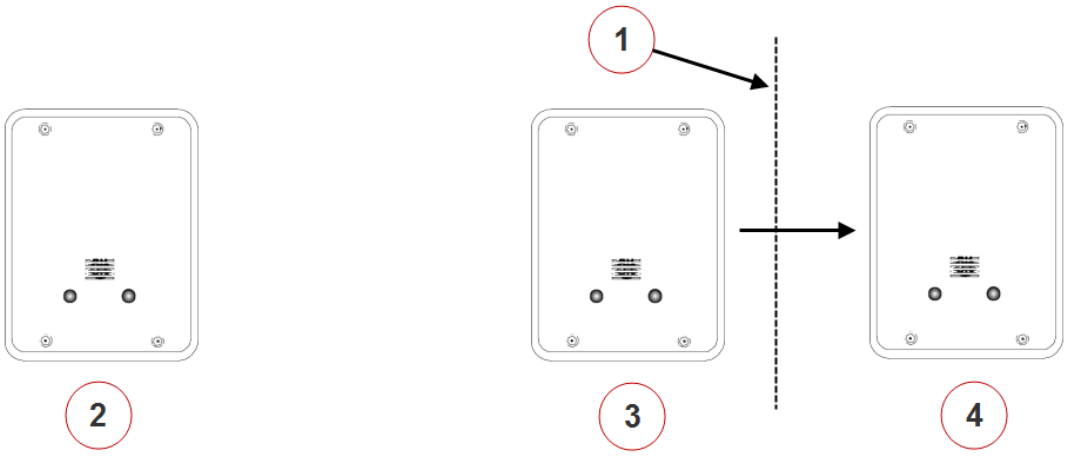


Figure 3.3: Receiver Spacing

1	Receiver 1 stops sounding the test beeps when receiver 2 is moved past this point	3	Receiver 2 at maximum range
2	Receiver 1	4	Receiver 2 beyond maximum range

Using a transponder, receivers, and laptop computer to determine receiver location

Notice!
System software and an area map must be installed on a laptop computer to use this method.

A transponder with long multiplex wires connected to receivers can be used to see actual alarm location before the receivers are placed. Place the receivers in the proposed locations wired back to the transponder. Program the receivers with their locations in the **Transponder Database**. Using the maintenance transmitter and the maintenance alarm database, activate alarm transmissions within the area surrounded by the temporarily placed receivers. Verify that the location accuracy is acceptable at all points of concern. If not acceptable move the receivers, update the receiver location in the **Transponder Database**, and retest. Do not test outside of the last receiver in any direction, as this gives incorrect locations. Repeat this test in all areas of different construction and concern at the site.

3.3.2 Indoor receiver installation

- Indoor receivers must be mounted in a evenly spaced grid no more than 25 m (80 ft) apart.
- Indoor receivers must be mounted 1.5 to 1.8 m (5 ft to 6 ft) above the floor. This is true even if this is a single story building. Do not mount receivers above the ceiling or in roof rafters.
- In multistory buildings, the receivers must be mounted directly above the receivers on the floor below. The same number of receivers must be used on each floor level. If you meet all of the indoor installation guidelines, you can expect the computed location to indicate the correct floor about 95% of the time.
- Receivers must not be mounted within 30 cm (1 ft) of any metal object, including wire mesh, metal foil, metal pipe and HVAC ducting in walls.

– Take care that large metal objects do not shield a receiver from a protected area. For example metal staircases, metal food serving lines, metal walls, lead lined walls, metal roofs, wire mesh in walls, walk-in freezers and refrigerators.

For the best indoor and outdoor location or an indoor only system

– Mount the indoor receivers on the recommended 25 m (80 ft) grid, with the last row of indoor receivers on the outside wall of the building. Do this even if the building is less than 25 m (80 ft) wide or long.
– There should be a receiver at each outside corner of a building.

Handling two protected buildings sharing a common wall with floor levels that do not match

– Ask the customer which building has areas of greater concern and favor the recommended mounting heights in that building.
– The recommended 25 m (80 ft) maximum indoor spacing grid should be maintained throughout both buildings as if the wall in question was not there. Mounting heights only for those receivers at or near (within 6 m [20 ft]) the wall in question should be affected. Mounting heights for all other receivers in the buildings must follow the indoor recommendation. Mark the recommended mounting height for receivers on the higher floor level and also mark the recommended mounting height for receivers on the lower floor level. Mount the receiver at its normal grid location midway between these two heights, but not above the ceiling level of the lower floor.

3.3.3 Outdoor receiver installation

– Outdoor receivers must be mounted in a evenly spaced grid no more than 90 m (300 ft) apart.
– Outdoor receivers must be mounted 3 m (10 ft) above the ground.
– Receivers must not be mounted within 30 cm (1 ft) of any metal object, including fences, metal walls and walls with wire mesh. If a receiver is mounted on a metal fence, that fence should be grounded (not floating or insulated from ground) and the receiver should be spaced 30 cm (1 ft) from the fence and 3 m (10 ft) above the ground.
– Take care that large metal objects do not shield a receiver from a protected area. For example; metal fences, metal staircases, metal buildings, power transformers and metal roofs.
– Receiver locations should be below building overhangs and eaves as these can shield the areas below them.
– Receivers should have a clear line of sight of the protected area. Therefore, take care where the ground is hilly or uneven, that there are no areas and low spots where several receivers can’t hear the signal.

Transition areas between indoor and outdoor areas

– An outside area directly between two buildings with complete indoor protection will need no additional receivers between the buildings, if they are 90 m (300 ft) or less apart.
– When protecting an outside area directly between two buildings with complete indoor protection, and they are more than 90 m (300 ft) apart, place a row of outside receivers evenly spaced between the buildings. Make sure the receiver row does not exceed the standard 90 m (300 ft) spacing from the buildings. The spacing between receivers in that row should be about the same as the spacing for the receivers in the buildings.

- Indoor receivers should be no more than 25 m (80 ft) apart and outdoor receivers should be no more that 90 m (300 ft) apart. Both of these recommendations work well in their respective areas. However, if a building is adjacent to an outdoor area, that building will have a greater density of receivers and, therefore, has a tendency to pull the computed location towards it. To counteract the building tendency to pull the location, consider the following special cases:
  - If the outdoor area adjacent to the building is wide open and the customer is not concerned about reduced location accuracy in this area, then nothing special needs to be done. Follow the normal indoor and outdoor recommendations.
  - The building is near the boundary of the protected area, with or without a fence at the boundary. The receivers in the building should be placed at the recommended 25 m (80 ft) spacing. The receivers at the boundary of the protected area near the building should be spaced about the same as those in the building, approximating the same grid as used in the building.
  - The building is adjacent to a large protected outdoor area that extends for more than 90 m (300 ft) from the building. The receivers in the building should be placed at the recommended 25 m (80 ft) spacing. The receivers in the large protected outdoor area should be placed on the normal 90 m (300 ft) grid except for the first row of receivers adjacent to the building. This first row of outdoor receivers in the transition area should “split the difference” between the indoor and outdoor spacing at about 60 m (200 ft).

Boundary areas at the outer edge of the protected area

The system cannot locate an alarm past the last receiver at the boundary of the protected area. Therefore, the last row of receivers must be at or past the end of the protected area.

3.4 Post construction setup

3.4.1 Testing the location accuracy of an installation

Notice!

Before doing any of the following testing, it is important to verify that every receiver in the system is functioning correctly using the procedure described in the Security Escort *Hardware Installation Manual*. Additionally, every receiver must be programmed in the **Transponder Database** with its actual physical location and floor level. **It is also important that receivers that are physically stacked directly above one another on floors of a building are also located at the same X and Y coordinates in the database**.

There are three methods that can be used to verify the location accuracy of an installed system, using a standard subscriber transmitter or using a maintenance transmitter. Repeat the chosen process throughout all protected areas. Ask the customer for the areas where they have special concerns and devote extra attention to those areas, since the customer is likely to be more critical in those areas.

Remember the intent of the Security Escort system is to dispatch a responding individual to an area that will not add additional delay to their response to that duress call. Therefore, the computed location should be considered to be in error only when it would add unacceptable additional time to the alarm response.

While testing, it is helpful to see which receivers are involved in the alarm response and the relative reception level they reported. To display the receivers, select menu **Utilities** > **Security Preferences**. Make sure the **No receiver icons** checkbox is not checked and click the **[Save]** button. Select menu **Setup > System Preferences**. If **Show test levels** and **Show maintenance levels** checkboxes are checked, the relative reception level is shown in the receiver icons; otherwise, the floor number will be shown.
When testing with any of the following methods, the transmitter must be used exactly as it would be used in normal operation. A transmitter designed to be belt mounted or used in a holster must be in its normal mounting attitude and be worn on the belt of the individual originating the test transmissions. Handheld transmitters must be held in the hand about waist high, never held above the head.

Using a standard subscriber transmitter

1. This method requires two people with radio contact between them. One person operates the computer running the Security Escort software, and the other takes the subscriber transmitter to the area to be tested.
2. Press the alarm on the transmitter and remain at the spot where you transmitted.
3. The computer operator acknowledges the alarm and accurately describes the computed location over the radio. The individual with the transmitter should confirm the reported location or describe over the radio the actual location. Either individual must record all discrepancies, including the actual and computed locations.
   We recommend using a map or floor plan and drawing an arrow from the actual alarm location to the reported location. It is also helpful if all successful alarm locations are marked with a **P** (passed), then the alarm can be reset from the computer screen.
4. For areas where there are alarm location problems, try facing in different directions in the same spot. Also generate additional alarms from different spots to fully understand the extent of the problem. You should generate alarms in areas adjacent to the area with the problem to see if they are also affected.

Using a maintenance transmitter with only one person

1. The Security Escort software retains the last 50 maintenance alarm locations. Make sure you are the only one using a maintenance transmitter on site, buddy check is off, and that you limit yourself to a maximum of 50 maintenance alarms per sequence.
2. Synchronize the time on your watch to the computer. Carry a detailed map or floor plan of the area to be tested that you can write on.
3. Take the maintenance transmitter to the area to be tested. Press the alarm on the transmitter and accurately mark the spot on the map where you transmitted with a “1” (for the first transmission). Also record the time of the first transmission only.
4. Continue to the next location, transmit and mark that spot on the map with a “2.” Repeat the process throughout the area to be tested, being sure not to exceed 50 alarm transmissions and making sure that at least 10-sec. elapse between transmissions.
5. When finished, return to the computer and select menu **File > Maintenance Alarm Database**. Scroll through the alarm list to find the alarm that matches the time of your first transmission. This is the maintenance alarm that you marked as “1” on your map.
6. Confirm that the actual location from the map matches the reported location.
7. If the actual location differs from the reported location, draw an arrow on the map from the actual location to the reported location. Press the up arrow once to go to the next alarm. Compare the locations, drawing an arrow to the reported location if they differ. Repeat this procedure for all points on your map, making sure that the points on the map

stop when you run out of entries in the scrolling list on the computer screen. Otherwise, the points on the map and the screen are out of sync and the errors on your map are incorrect and misleading.

8. For areas where there were alarm location problems, you may want to repeat the process above facing different directions from the same spot. This generates additional alarms from different spots in the problem areas to fully understand the extent of the problem.
9. You should also generate alarms in areas adjacent to the area with the problem to see if they are also affected.

Using a maintenance transmitter with two people

1. The two people must have radio contact between them. One person operates the computer running the Security Escort software and the other takes the maintenance transmitter to the area to be tested.
2. At the computer select menu **File > Maintenance Alarm Database**. Make sure the top item in the scrolling list is selected.
3. Press the alarm on the transmitter and remain at the spot where you transmitted. At the computer, observe the alarm and accurately describe the computed location over the radio. The individual with the transmitter should confirm the reported location or describe the actual location over the radio. Either individual must record all discrepancies, including the actual and computed locations. We recommend using a map or floor plan and drawing an arrow from the actual alarm location to the reported location. It is also helpful if all successful alarm locations are marked with a **P** (passed).
4. For areas where there are alarm location problems, try facing in different directions from the same spot.
5. Generate additional alarms from different spots to fully understand the extent of the problem.
6. You should generate alarms in areas adjacent to the area with the problem to see if they are also affected.

Reviewing potential problem areas

Review the potential problem areas on the maps with the customer to see which areas cause them concerns, and which areas they consider acceptable. If the customer considers an area acceptable, it is typically not worth spending additional time trying to improve the location accuracy in those areas.

3.4.2 Improving the location accuracy of an installation

Once we have identified those areas that must be improved, what are the options to improve the computed location accuracy?

Notice!

All changes using the following steps could potentially change the computed locations for all alarms at or around the changed area. Therefore, after any change is made, the entire vicinity around the changed area must be verified.

– Typically the first thought is to add more receivers in the problem area. Generally this is a bad approach. If the system was properly designed using the recommended grid layout, adding extra receivers in any area of the grid will distort the response in adjacent areas and floors. While it may seem to fix the problem area, typically it will create more problems in adjacent areas. The exception is when an area is shielded by something such

as wire mesh in the walls that prevent the RF transmitted signal from passing through. Therefore, additional receivers may have to be added in the shielded area to ensure that all alarm transmissions will be heard.

- Verify that the location of the receivers in the **Transponder Database** is accurate to their physical location, and the receivers are indicated to be at the correct floor level. It is also important that receivers that were physically stacked directly above one another on floors of a building are also located at the same X and Y coordinates in the database.
- Try changing the **Transponder Database** location of receivers (not the actual physical location) one at a time while testing the alarm location response, using one of the testing methods above. For example, if alarms are getting pulled outside a building in one area, move the closest receiver (in the **Transponder Database**) to that area a little further into the building and retest. If the area can be corrected using this method, verify the surrounding areas to make sure they were not adversely affected. It is generally 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.
- Starting with version 2.03 and higher, the Security Escort software allows 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. Try changing the **Transponder Database** sensitivity of receivers one at a time while testing the alarm location response, using one of the testing methods above. 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. **It is generally 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**.
- Starting with version 2.03 and higher 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 Security Escort algorithm), “Linear”, “Low“ pull, “Medium” pull and “Strong” pull. By default, when a receiver is set for outside or tunnel, it will use the “Linear” algorithm and all other receivers will use the “Low” pull algorithm. The receiver that hears the alarm transmission the strongest will determine the algorithm used for this alarm. Changing the **Transponder Database** algorithm setting for a receiver only affects the location when the alarm is close to this receiver and it hears the alarm the strongest. Change the **Transponder Database** algorithm setting for a receiver and test in its area, using one of the testing methods above. The stronger the pull the more the alarm will be pulled towards the receiver, with “Linear” having no extra pull. Verify the surrounding areas to make sure they have not been adversely affected.
- Starting with version 2.03 and higher of the Security Escort software, the five different location algorithms can individually limit how close other receivers must be to the level of the receiver hearing the alarm the best, before they will be included in the alarm. “Classic” (original Security Escort algorithm), “Linear”, “Low” pull, “Medium” pull and “Strong” pull each have a separate setting. By adjusting this setting you can control if distant receivers with low receive levels will be considered in the alarm calculation.
- Starting with version 2.03 and higher 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. 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 may pull towards the

building. The “Virtual” receiver references to other physical receivers that must be on the same transponder. Only if both of the referenced receivers receive an alarm transmission, then the “Virtual” receiver will be added to the alarm as if was a physical receiver that heard the alarm at the average receive level of the two reference receivers.
The “Virtual” receiver’s location and sensitivity may be adjusted the same as a physical receiver. After a “Virtual” receiver is added, verify the surrounding areas to make sure they have not been adversely affected. **In no event should a “Virtual” receiver be utilized as a cost savings measure to avoid the installation of an actual receiver**.

4 Installation instructions

4.1 Overview of installation process

This section includes information about the installation and setup of the individual components and system wiring. It is recommended that the installation instructions that accompany each specific component be consulted prior to beginning any phase of the installation.

A typical installation proceeds in the following order:

1. The Site Survey is completed, indicating the proposed location of each component.
2. Wiring runs to all of the proposed component locations and the central console.
3. Empty enclosures are installed as specified in the Site Survey.
4. The components are secured inside the enclosures and connected to the previously run wiring. The individual components are set up and their addresses recorded.

Notice!
Use the *Transponder Information Sheet*, located in the *Appendix* of this document, to keep track of receiver and alert unit addresses and location for programming the Transponder Database.

5. The recorded addresses are entered into the central console and the system is brought on-line.
6. The system is tested and tuned up as needed.

4.2 Run system wiring

4.2.1 General guidelines

After the site survey (and special pre-construction verifications) has been completed, the wiring can be run between the proposed locations of the system components and the Central Console. See specific installation instructions accompanying each component for wiring details.

The following table indicates the specifications for the wiring:

Application		Diagram Ref	Gauge	Conductors	Maximum Distance	Notes
From	To					
Transponder	Transformer	1	1.5 mm (16 AWG)	2	15 m (50 ft)	Standard lamp cord
	Alert Unit	2	1.2 mm (18 AWG)	4	900 m (3000 ft) per bus	Solid, not twisted, not shielded
	Receiver	2	1.2 mm (18 AWG)	4	900 m (3000 ft) per bus	Solid, not twisted, not shielded

Application		Diagram Ref	Gauge	Conductors	Maximum Distance	Notes
From	To					
	SE485	3	0.5 mm (24 AWG)	4 wire, 2 twisted pair	See Transponder – SE485 Wiring table.	**IMPORTANT!** Must be twisted pair, not shielded. CAT5 cable preferred.
	Siren/Strobe	4	1.2 mm (18 AWG)	4	15 m (50 ft)	Solid, not twisted, not shielded
Alert Unit	Transformer	5	1.5 mm (16 AWG)	2	15 m (50 ft)	Standard lamp cord
	Siren/Strobe	6	1.5 mm (18 AWG)	4	15 m (50 ft)	Solid, not twisted, not shielded

Tab. 4.4: Wiring Guidelines

* See the corresponding numbers in Figure 4.5, Figure 4.6, and Figure 4.7.

Number of Transponders	Maximum Wire Length
1 to 4	6100 m (20000 ft)
8	3050 m (10000 ft)
12	1525 m (5000 ft)
16	900 m (3000 ft)

Tab. 4.5: Transponder – SE485 Wiring Table

4.2.2 Observe established standards

Install cable according to local code requirements. In the USA, refer to *the National Electrical Code Standards*, located *in Chapter 8 Article 800* of the *National Electrical Code*, and applicable local and regional codes.

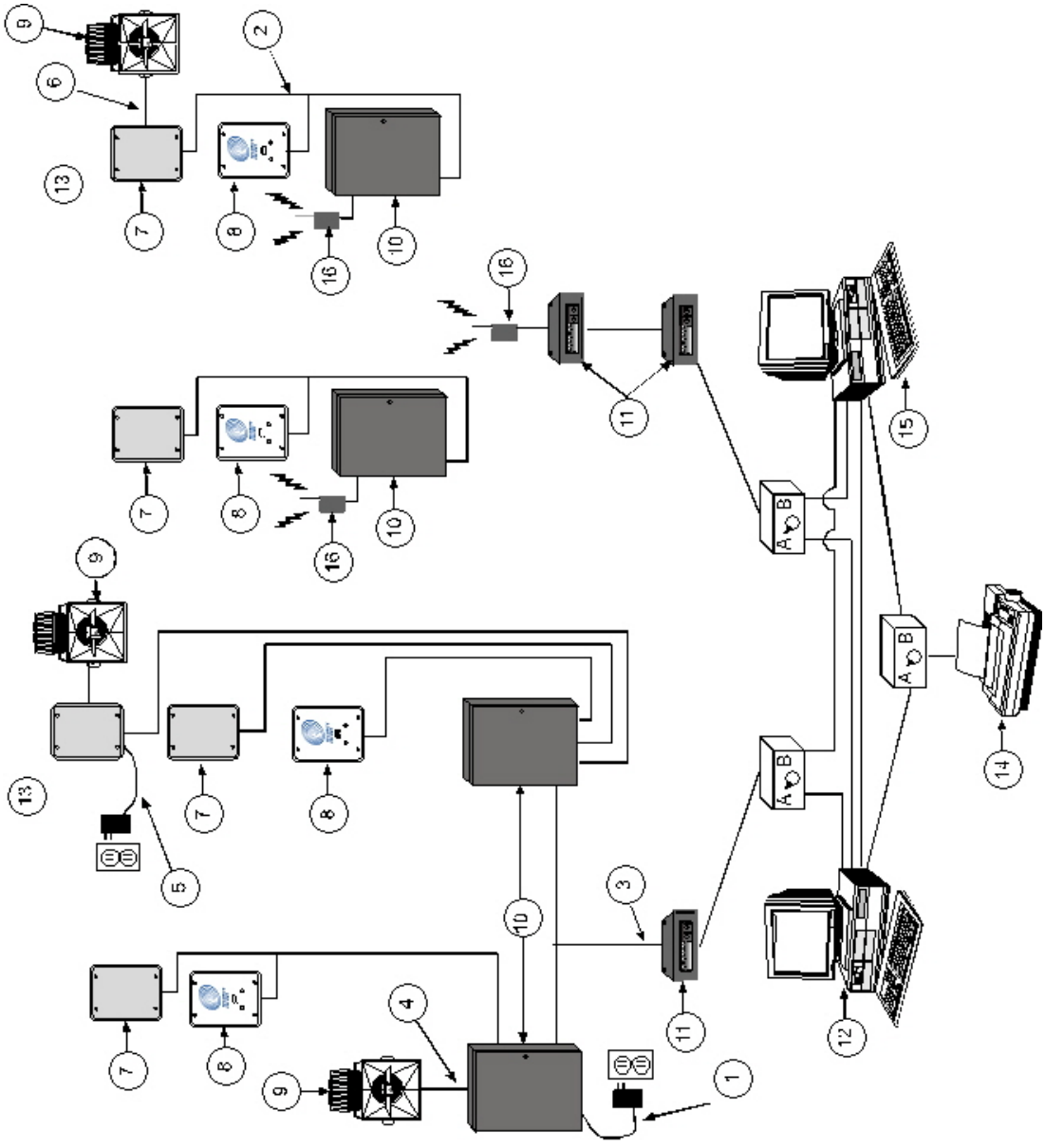


Figure 4.1: General Wiring Diagram

1	Wiring guidelines	9	Siren/strobe
2	Wiring guidelines	10	Transponder
3	Wiring guidelines	11	SE485 Interface **
4	Wiring guidelines	12	Central console computer # 1 (primary)
5	Wiring guidelines	13	Alert unit
6	Wiring guidelines	14	Printer
7	Outdoor receiver	15	Central console computer # 2 (back-up)
8	Indoor receiver	16	ProxLink

* See Transponder - SE485 Wiring Table for wiring details
** SE485 Interface units are only needed if the length of the cable between the console and the ProxLink is greater than 15 m (50 ft)

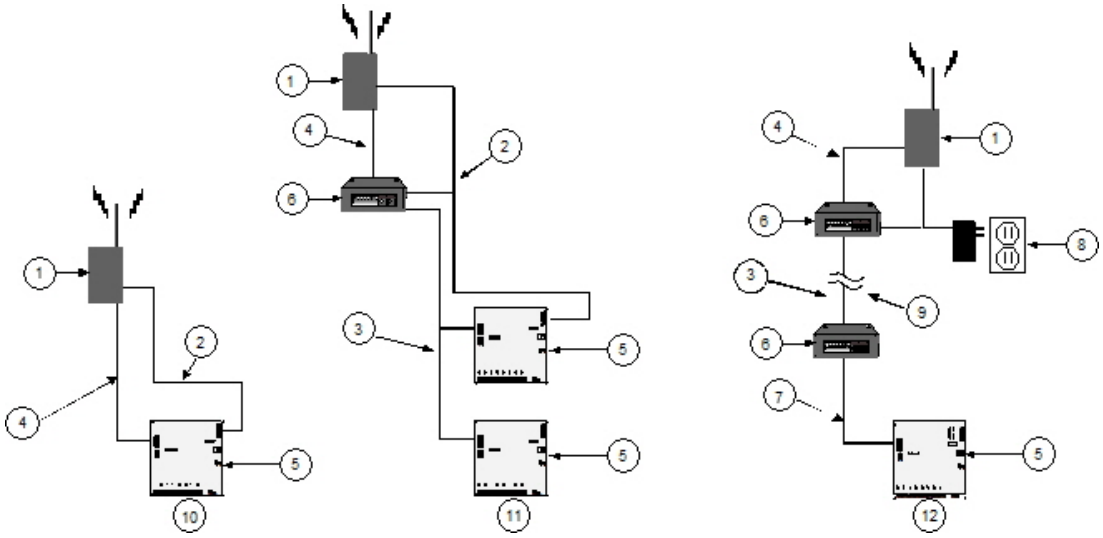


Figure 4.2: Transponder to ProxLink Wiring

1	ProxLink	7	Serial Cable
2	C312 Power Cable	8	Requires backup power
3	Wiring guidelines *	9	15 m (50 ft) or greater
4	C312 Data Cable	10	ProxLink to Transponder 0 m to 15 m (0 ft to 50 ft)
5	Transponder	11	Transponders to one ProxLink 0 m to 15 m (0 ft to 50 ft) multiple
6	SE485 Interface	12	Central console computer # 1 (primary)

* See Transponder - SE485 Wiring Table for wiring details

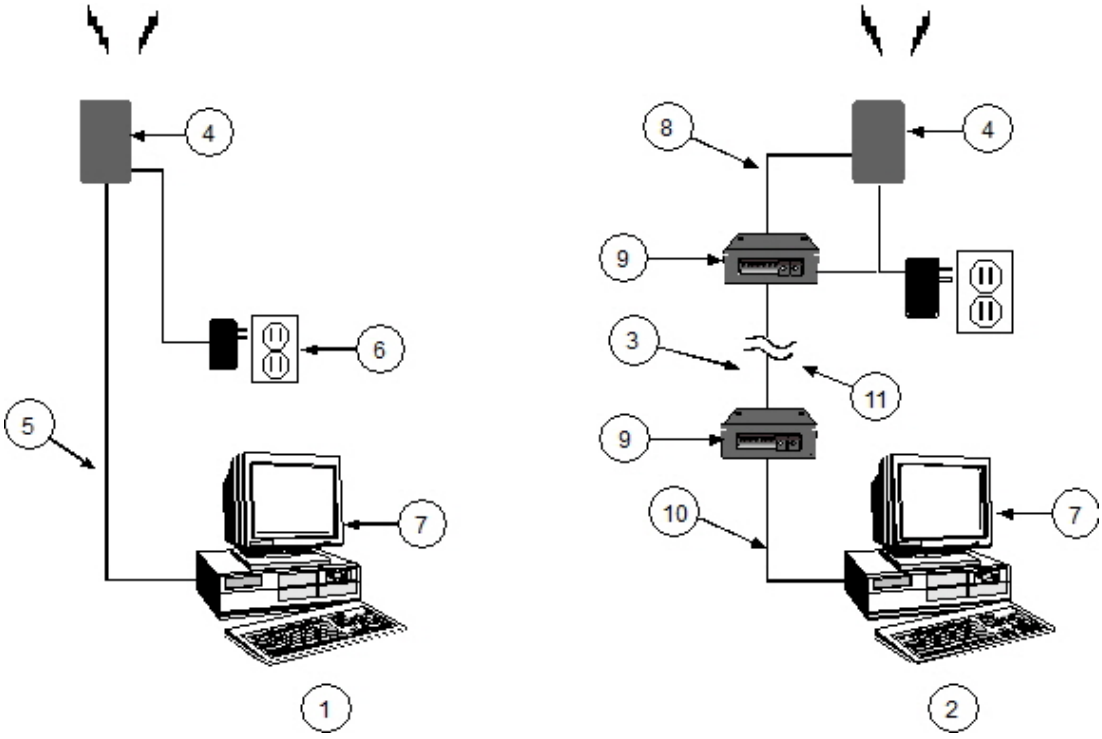


Figure 4.3: ProxLink to Central Console

1	ProxLink to computer 0 m to 15 m (0 ft to 50 ft)	7	Central console computer (requires back-up power)
2	ProxLink to computer 15 m (50 ft) or greater	8	C312 Data Cable
3	Wiring guidelines *	9	SE485 Interface
4	ProxLink	10	Serial cable
5	ProxLink Data Cable 9 to 25 pin (supplied with ProxLink)	11	15 m (50 ft) or greater
6	Requires back-up power		

* See Transponder - SE485 Wiring Table for wiring details

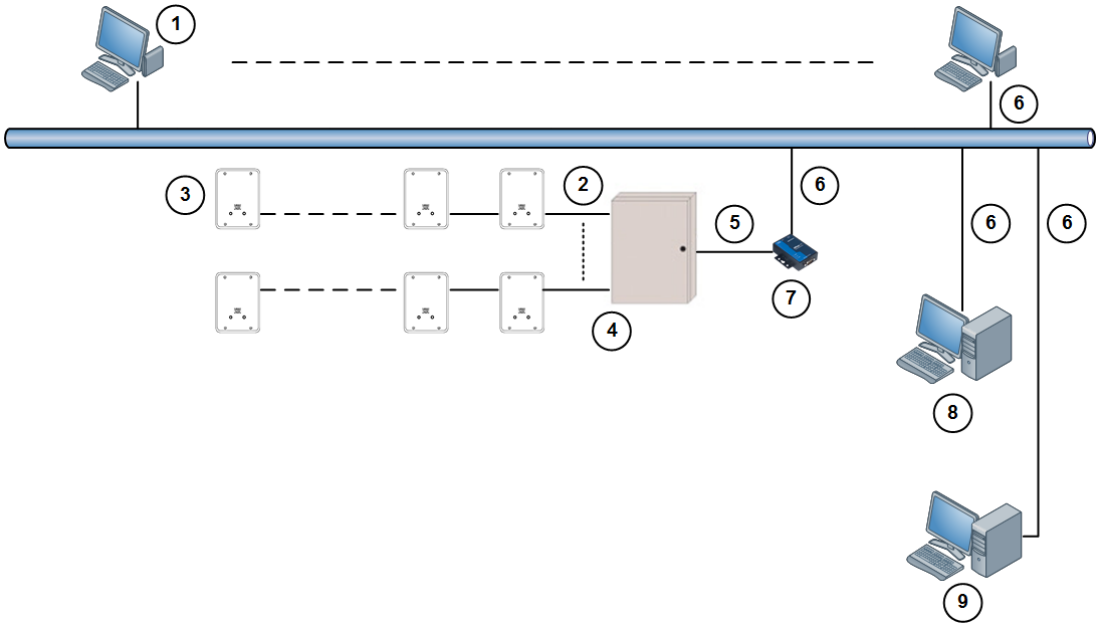


Figure 4.4: Transponder to Moxa Interface

1	Workstation computer	6	Ethernet cable
2	Wiring guidelines *	7	Moxa device
3	Receiver	8	Slave computer
4	Transponder	9	Central Console (master computer)
5	Serial cable 9 pin male to 9 pin female (standard)		

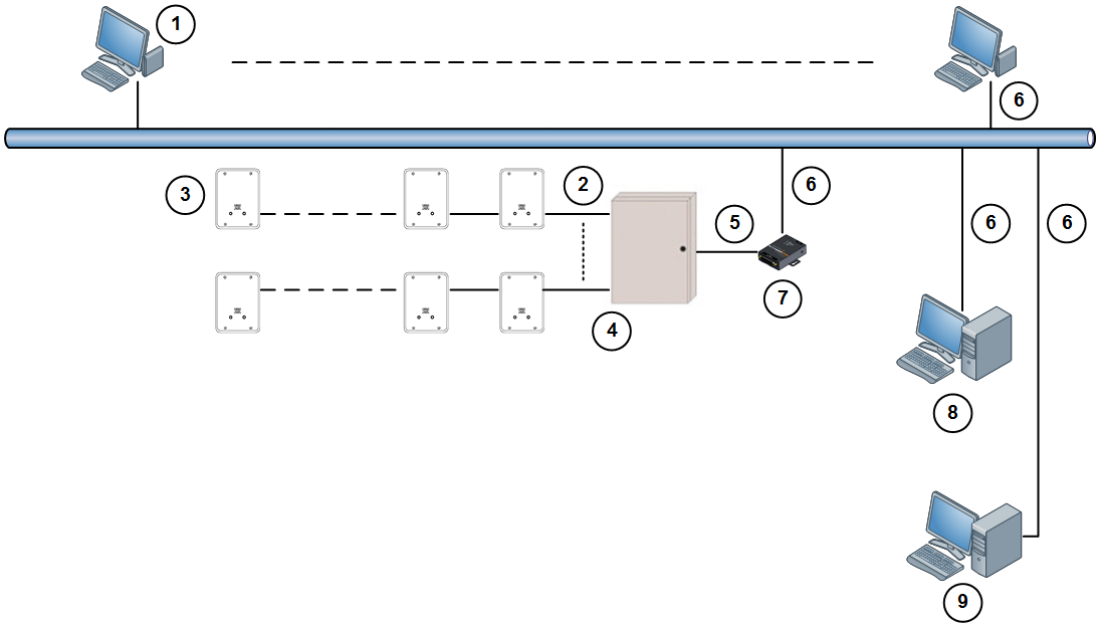


Figure 4.5: Transponder to Lantronix Interface

1	Workstation computer	6	Ethernet cable
2	Wiring guidelines *	7	Lantronix device
3	Receiver	8	Slave computer

4	Transponder	9	Central Console (master computer)
5	Serial cable 9 pin male to 25 pin male (modified)		

4.2.3 Transponder wiring notes

- Wiring to receivers and alert units can be home-run (individual), daisy-chain (from device to device), or a combination of both. T-Tapping is okay. The recommended cable is shown in Wiring Guidelines table.
- Due to communications limitations between the transponder and receivers, a maximum of 200 supervised SE2 transmitters can be handled in a Security Escort system.

Notice!
How can you increase the number of supervised transmitters that can be handled in a Security Escort system? In general, using more transponder buses with fewer receivers per bus helps. The transponder can process all the receivers at the same receiver address on different buses at the same time. To handle higher volumes of traffic, assign all of the receivers likely to hear a supervision transmission to the same receiver bus address on different buses. In an installation where four receivers hear each supervision transmission, the number of transmitters can be doubled when all of the receivers hearing a transmission are the same address on different buses. If you have any questions, contact Bosch Security Systems Technical Service at the number on the back cover of this manual.

- Wiring from SE485 to transponders can be home-run (individual), daisy-chain (from device to device), or a combination of both. T-Tapping is okay. The recommended cable is shown in Wiring Guidelines table.

Notice!
The cable between the SE485 and the transponder must be twisted pair communication cable.

4.2.4 Receiver wiring notes

For applicable wiring notes, see *Transponder wiring notes, page 35*.

4.2.5 Alert unit wiring notes

- Battery cables (see *System components description, page 7*)
- AC Power (see *General guidelines, page 29*)
- Siren (see *General guidelines, page 29*)
- Strobe (see *General guidelines, page 29*)
- Bus (see *Transponder wiring notes, page 35*)

4.2.6 Moxa interface wiring notes

- The Moxa device must be powered at all times. Use the included power adapter.
- A standard male DB9 to female DB9 serial cable is used to connect the transponder to the Moxa device.
- Instructions on setting up the Moxa device is based on the recommended model NPort 5150 (firmware version: 3.4 Build 11080114).

The pinouts of male DB9 serial port of Moxa NPort 5150 are as follows:

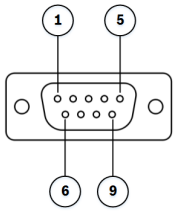


Figure 4.6: Moxa NPort 5150 Male DB9

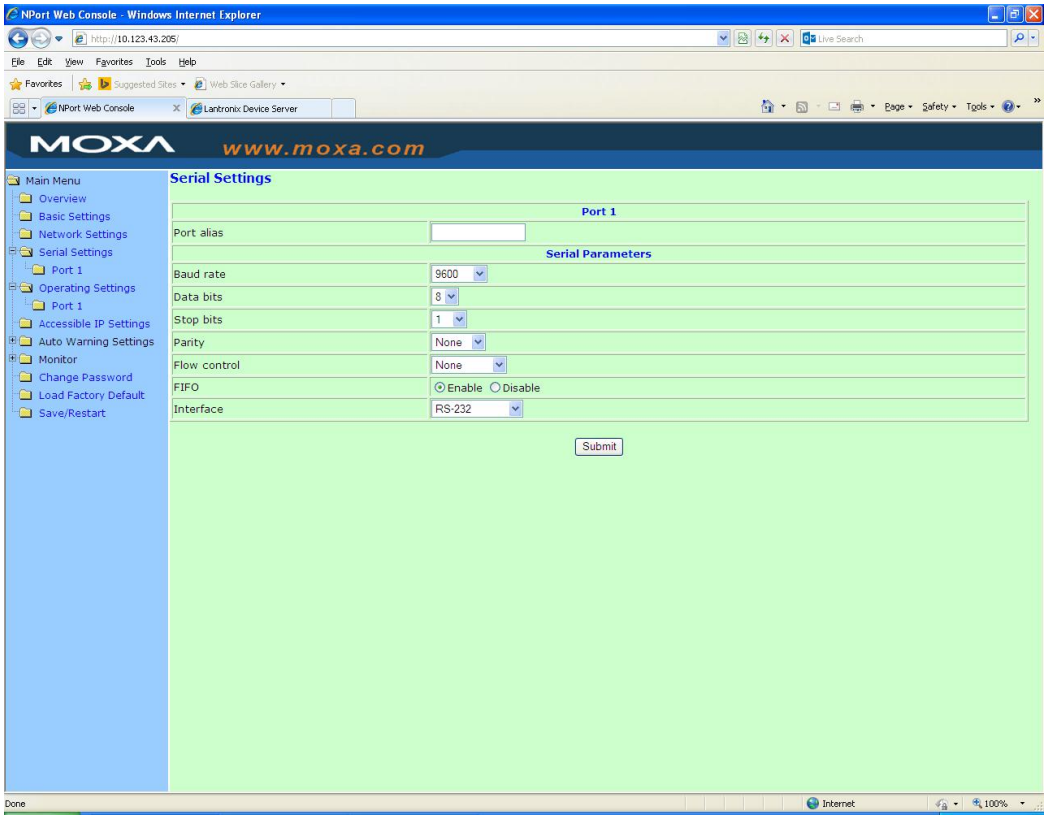
Pin Number	RS-232	RS-422/RS-485 (4W)	RS-485 (2W)
1	DCD	TXD-(A)	--
2	RxD	TXD+(B)	--
3	TxD	RXD+(B)	Data+(B)
4	DTR	RXD-(A)	Data-(A)
5	GND	GND	GND
6	DSR	--	--
7	RTS	--	--
8	CTS	--	--
9	--	--	--

Notice!
Third party user interfaces are subject to change without notice at the sole discretion of the respective providers but configuration setting shall remains as specified.

Follow the instructions below to set up the NPort 5150 device and use the serial cable to connect the transponder to the Ethernet network.

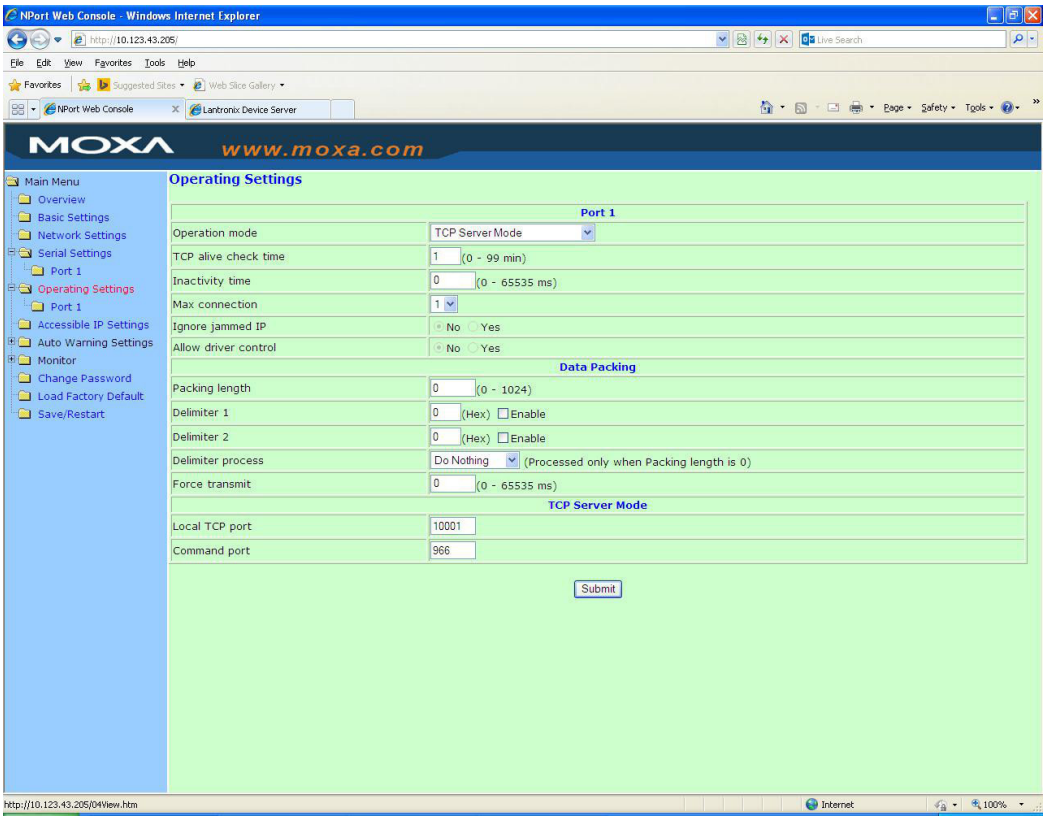
1. Connect NPort 5150 to the Ethernet network.
2. Set up and configure the IP address of the Moxa device. There are several methods to configure the IP address. Please refer to the *Moxa User Manual* on steps to configure the IP address.
3. From a computer on the Ethernet network, login to the Moxa device using the web browser interface.

4. Go to **Serial Settings** > **Port 1**. Remove any entry in the **Port alias** field (it must be empty). Set the **Baud Rate** field as “9600”, the **Data Bits** field as “8”, the **Stop Bits** field as “1”, the **Parity** field as “None”, the **Flow Control** field as “None”, the **FIFO** field as “Enable” and the **Interface** field as “RS-232”.



5. Click the **[Submit]** button to make the changes and restart the Moxa device.
6. Go to **Operating Settings** > **Port 1**. It is recommended (depending on the setup environment) to enter “1” in the **TCP alive check time** field, “0” in the **Inactivity time** field, and “0” in the **Force transmit** field. Please refer to the *Moxa User Manual* for further details. Enter the port number of the transponder in the **Local TCP Port** field. This port

number must be the same number as the one that is set for the transponder in the **Transponder Database** of the Security Escort software.



7. Click the **[Submit]** button to make the changes and restart the Moxa device.
8. The connecting cable is a male DB9 to female DB9 serial cable. Connect the male DB9 connector to the transponder and the female DB9 connector to the Moxa device.

4.2.7 Lantronix interface wiring notes

- The Lantronix device must be powered at all times. Use the included power adapter.
- Do not use the female DB9-to-male DB25 serial cable included. A modified serial cable must be used to connect the transponder to the Lantronix device.
- Instructions on setting up the Lantronix device is based on the recommended model UDS1100.

The pinouts of female DB25 serial port of Lantronix are as follows:

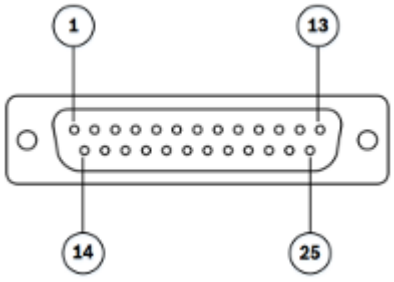


Figure 4.7: Lantronix UDS1100 Female DB25

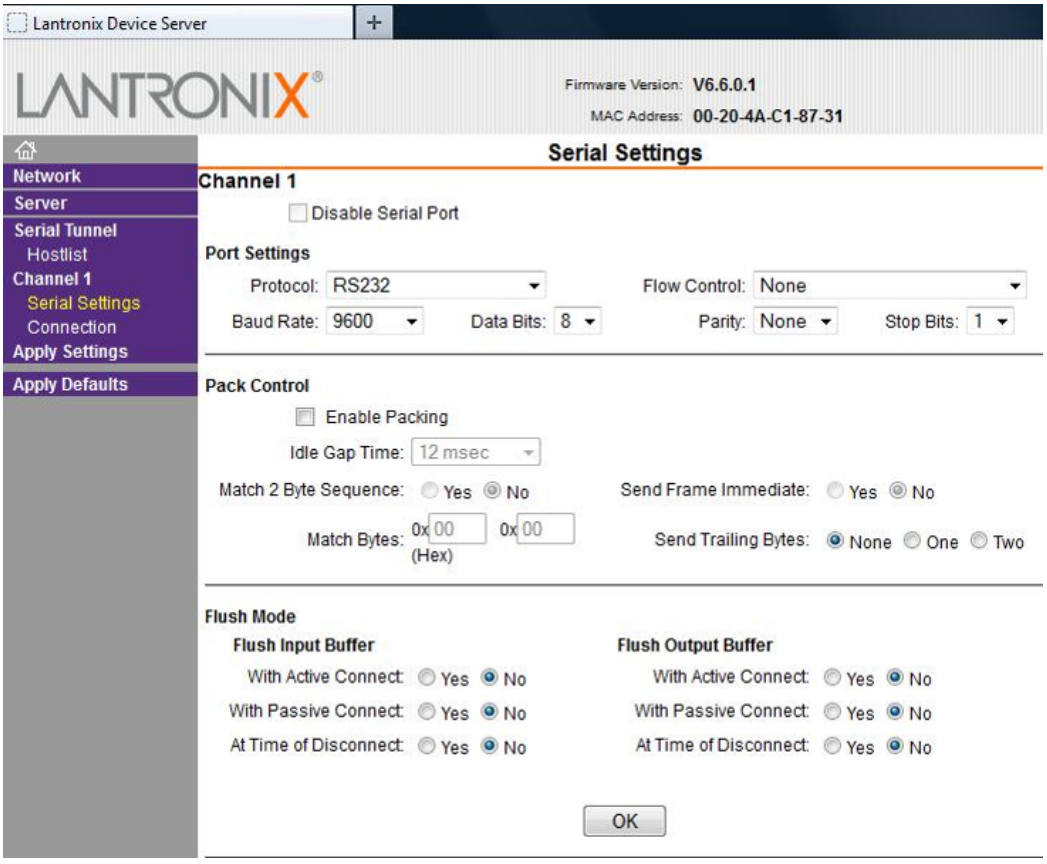
Pin Number	RS-232 Signals
1	Chassis Ground
2	Transmit Data
3	Receive Data
4	Request to Send
5	Clear to Send
6	Data Set Ready
7	Signal Ground
8	Carrier Detect
9	---
10	---
11	Receive Clock Out
12	---
13	---
14	---
15	Transmit Clock In
16	---
17	Receive Clock In
18	Local Loopback
19	---
20	Data Terminal Ready
21	Remote Loopback
22	---
23	---
24	Transmit Clock Out
25	Test Mode

Notice!
Third party user interfaces are subject to change without notice at the sole discretion of the respective providers but configuration setting shall remains as specified.

Follow the instructions below to set up the UDS1100 device and modify the serial cable to connect the transponder to the Ethernet network.

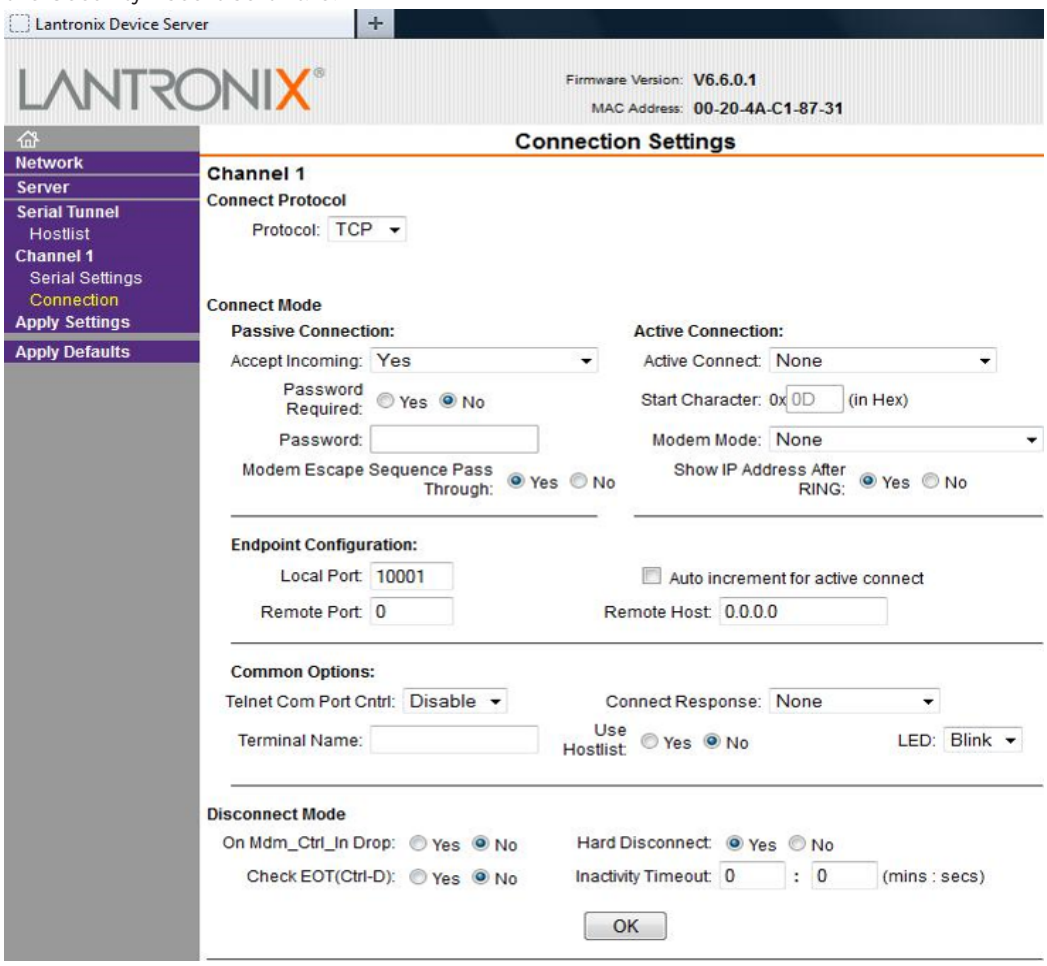
1. Connect UDS1100 to the Ethernet network.

2. Set up and configure the IP address of the Lantronix device. There are several methods to configure the IP address. Refer to the Lantronix User Guides on steps to configure the IP address.
   Connect the Lantronix device to the Ethernet network.
3. From a computer on the Ethernet network, login to the Lantronix device using the web browser interface with the default user ID and password.
4. Go to **Channel 1** > **Serial Settings**. Configure the **Protocol** field as “RS232”, the **Flow Control** field as “None”, the **Baud Rate** field as “9600”, the **Data Bits** field as “8”, the **Parity** field as “None”, and the **Stop Bits** field as “1”.



5. Click the **[OK]** button to apply the settings,

6. Go to **Channel 1** > **Connection**. Select “TCP” from the drop down list of **Protocol** field. Enter the port number of the transponder in the **Local Port** field. This port number is the same number as the one that is set for the transponder in the **Transponder Database** of the Security Escort software.



7. Click the **[OK]** button to apply the settings.
8. The connecting cable is a modified male DB9 to male DB25 serial cable. Only 3 wires are compulsory for the modification of DB9 to DB25 cable as illustrated in the table below.

RS232 Pin Assignment	
DB9 Pin Male	**DB25 Pin Male**
Pin	**Pin**
2	**2**
3	**3**
5	**7**

Tab. 4.6: Wiring – Required pins

9. Connect the male DB9 connector to the transponder and the male DB25 connector to the Lantronix device.

4.2.8 SE485 interface wiring notes

– For Security Escort system to maintain operation, the SE485 must be powered at all times. Use the included 9 V adapter, plugged into an Uninterrupted Power Supply (UPS). The SE485 can also be powered from the transponder's 9 V output connected to the 9 V DC input wiring connectors.
– Up to four SE485s can be connected to the central console not counting pairs to ProxLink radios. If using multiple SE485s, use the expansion power connector cable provided with the SE485 package.

Notice!
The cable between the SE485 and the transponder must be twisted pair communication cable, not shielded. CAT 5 cable is recommended.

4.3 Mounting the enclosures

4.3.1 AE1 small indoor enclosure

The AE1 enclosure houses the EA500 transponder or the alert unit. It is suitable only for indoor installation. See *AE1, Small Indoor Enclosure, page 16* for specifications.
Mount the enclosure in a secure location away from excessive heat and moisture.

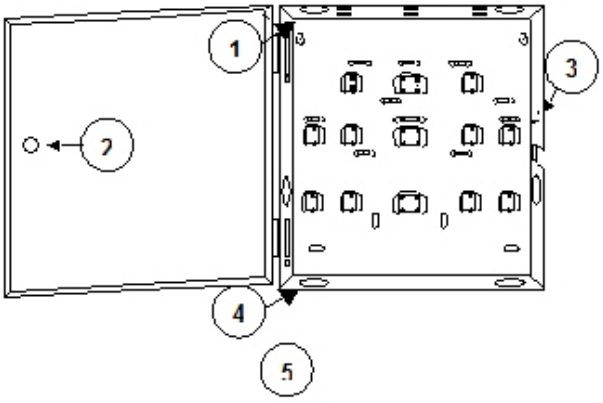


Figure 4.8: AE1 Enclosure

1	Flip-up view to show retainer tabs	4	Wire entrance (6)
2	Hole for lock and key assembly	5	Inside of AE1 enclosure
3	Place tamper switch here. Use the three longer screws to secure.		

4.3.2 AE3 large indoor enclosure

The AE3 large indoor enclosure houses the transponder. It is suitable only for indoor installation. See *AE3, Large Indoor Enclosure, page 16* for specifications.
Mount the enclosure in a secure location away from excessive heat and moisture.

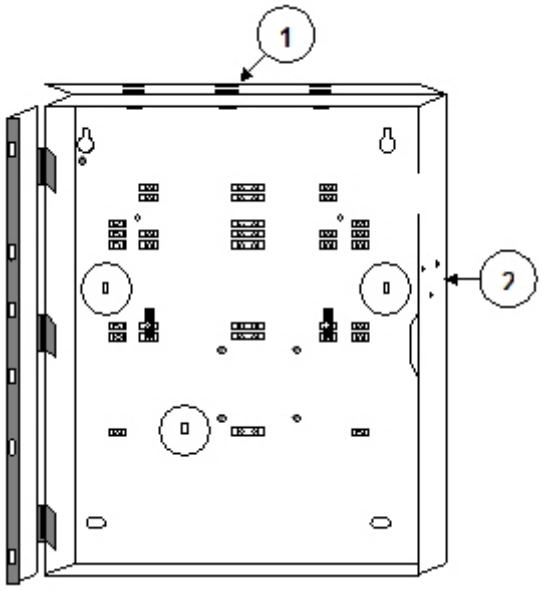


Figure 4.9: AE3 Enclosure

1	View to show retainer tabs.	2	Tamper switch mounts here.

4.3.3 AE100 indoor enclosure

The AE100 indoor enclosure houses the receiver. It is suitable only for indoor installation. See *AE100 Indoor Enclosure, page 17* for specifications. Use the security hex driver to secure the face of the enclosure to the body.

Notice!
Refer to the EA102 *Installation Instructions and Site Survey* for specifications and methods for achieving optimum receiver placement.

When mounting the enclosure to a pre-wired electrical box, make sure that the electrical box has a 15 cm (6 in) overhead clearance. The enclosure should be mounted as shown in the figure below.

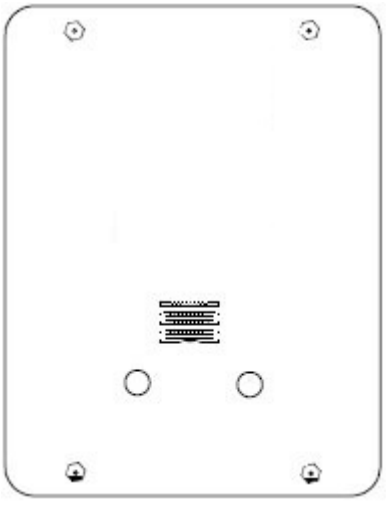


Figure 4.10: AE100 Enclosure

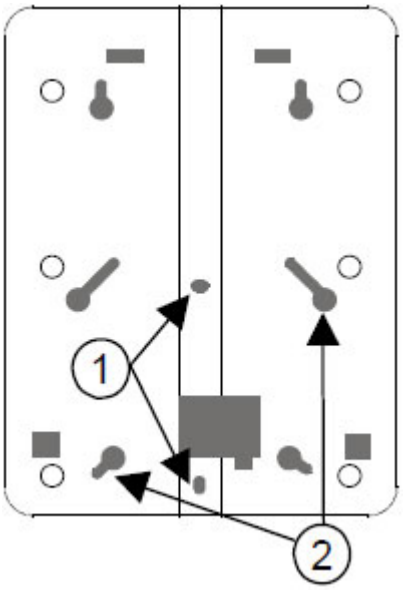


Figure 4.11: Back of AE100 Enclosure

1	Use with single-gang electrical boxes.	2	Use with 9 cm (3.5 in) square electrical boxes.

Notice!
The enclosure does not currently support octagonal electrical boxes.

4.3.4 AE101 outdoor enclosure

This enclosure houses the receiver or alert unit. It is suitable for outdoor installation. See *AE101 Outdoor Enclosure, page 17* for specifications.

Notice!
Do not use this enclosure if you intend to allow user feedback through the sounder and LEDs of the receiver.

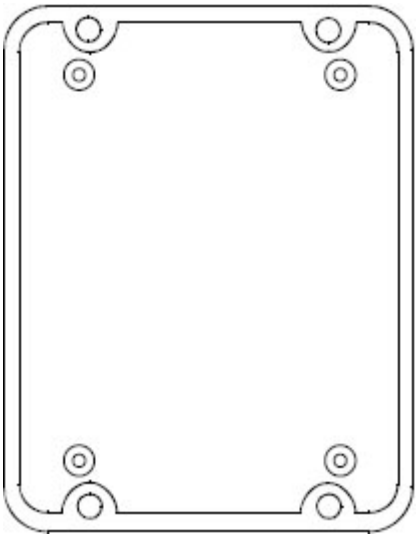


Figure 4.12: Inside AE101 Enclosure

4.4 Mounting and setting up components

4.4.1 EA102 receiver installation

Mounting

Mount the electronic assembly to the enclosure. Leave at least 10 cm (4 in) of wire hanging out of the unit. Do not leave extra wire inside the enclosure as this could impact the receiving antennas.

Set the Address

Every module on each multiplex bus of the transponder must have its own address. Set the address on the alert unit using the address switch. See the *EA102 Installation Instructions*. Use only address numbers 0 through 7. Do NOT use address numbers 8 and 9.

4.4.2 EA500 transponder installation

Mounting

Mount the electronic assembly to the enclosure using the hardware kit provided. See figures below for mounting location.

Set the Address

Every transponder in the system must have a unique address. Set the address on the transponder using the DIP switches in the upper-right corner. Use the chart included in the transponder's *Installation Guide* for the correct address settings.

Wiring

- Connect the bus wires.
- Connect the tamper switch wires.
- Connect the serial cable or SE485 wires (set the proper switch position).
- Connect the output siren/strobe if used.
- Connect the keyswitch if used.
- Connect 9 V output to ProxLink or SE485 if used.

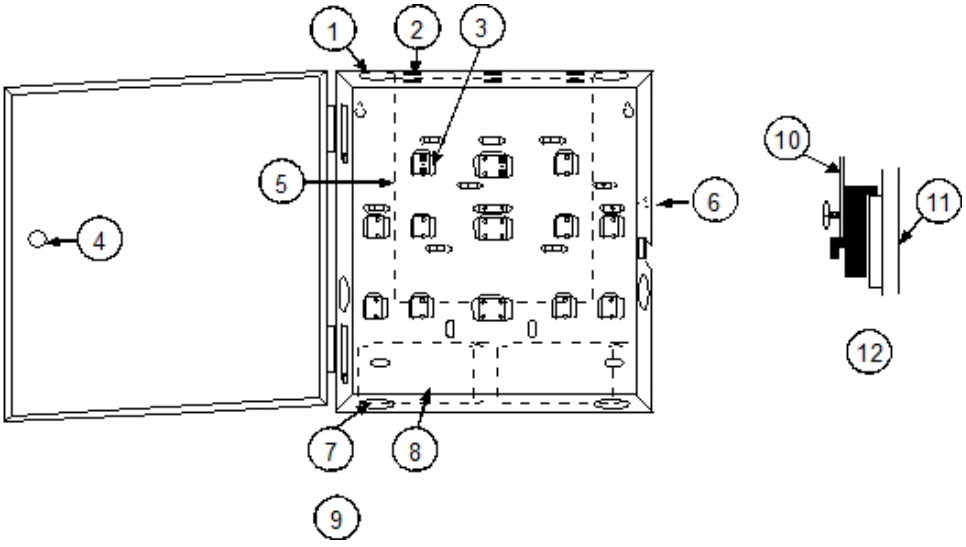


Figure 4.13: EA500 Mounting to AE1 Enclosure

1	Flip-up view to show retainer tabs	7	Wire entrances (6)
2	Slide board in-between retainer tabs	8	Outline of battery location (1 or 2)
3	Place board over support posts, use two of smaller screws to secure	9	Inside of AE1 Enclosure
4	Hole for lock and key assembly	10	Circuit board
5	Outline of where to mount circuit board	11	Enclosure
6	Place tamper switch here. Use the three longer screws to secure	12	Support Post Assembly

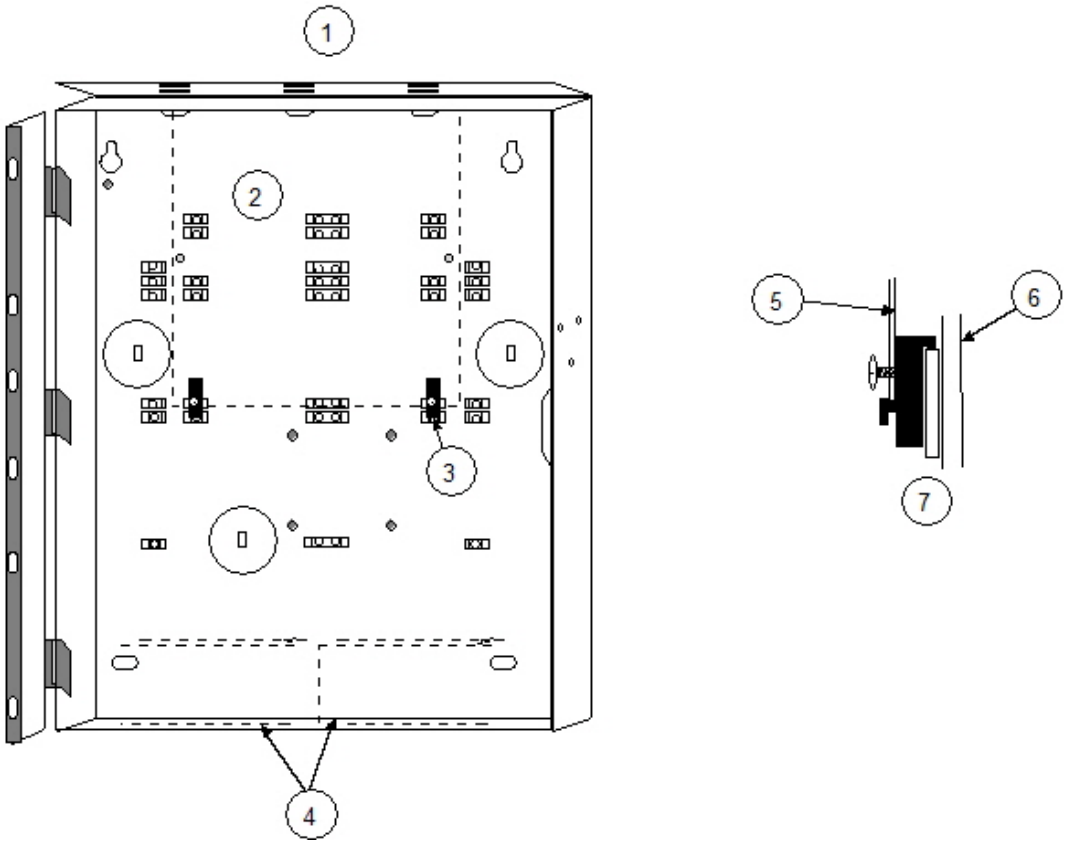


Figure 4.14: EA500 Mounting to AE3 Enclosure

4.4.3 EA120 alert unit installation

Mounting

The alert unit should be mounted indoors; however, an outdoor enclosure is available. The horn/strobe should always be mounted outdoors.

Mount the circuit board to the enclosure as indicated in the figures below.

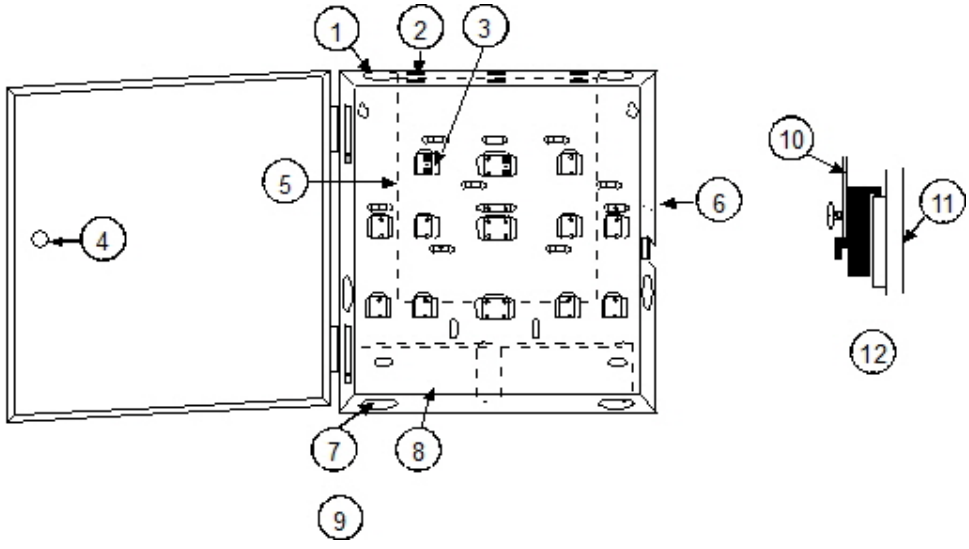


Figure 4.15: Mounting the EA120 to the AE1 Enclosure

1	Flip-up view to show retainer tabs.	7	Wire entrances (6)

2	Slide board in-between retainer tabs.	8	Outline of battery location (1 or 2)
3	Place board over support posts, use two of smaller screws to secure.	9	Inside of AE1 enclosure
4	Hole for lock and key assembly.	10	Circuit board
5	Outline of where to mount circuit board.	11	Enclosure
6	Place tamper switch here. Use the three longer screws to secure.	12	Support post assembly

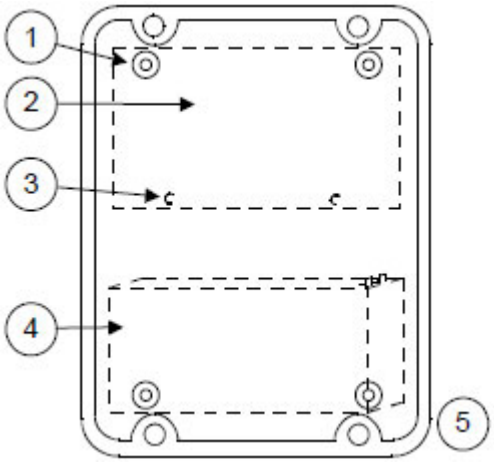


Figure 4.16: Mounting the EA120 in the AE101 Enclosure

1	Use the two plastic screws here.	4	Outline of where to place battery (only 3 Ah battery fits.)
2	Outline of where to mount circuit board.	5	Inside the AE101 enclosure.
3	Insert the stand-offs into these holes, then stick to the inside of the enclosure.		

Wiring

The alert unit gets its main power (for horn/strobe activation) from the 18 V AC transformer and its backup power from a battery. However, the multiplex bus continues to supply the transponder information on status and troubles in the event local power is lost.

– Connect bus wires.
– Connect siren/strobe wires.
– Connect tamper wires, if used.

Set the Address

Every module on each multiplex bus of the transponder must have its own address. Set the address on the alert unit using the address switch. See the *EA120 Installation Instructions*. Use only address numbers 0 through 7. Do NOT use address numbers 8 and 9.

4.4.4 ProxLink setup

Configuration procedure

Notice!
For more details refer to the *ProxLink Radio Module User's Manual*

Required equipment

– ProxLink Radio Module
– PC with RS-232 port running a terminal emulation software package. Select **Start > Programs > Accessories > Hyper Terminal**.
– ProxLink DB-9 to DB-25 Female RS-232 Cable
– 9 V DC Power Supply

Configure

Select one of seven radio channels (902 MHz to 928 MHz). Make certain that the channel chosen is the same for all the ProxLink located at the transponders and for the ProxLink at the Central Console computer.
Select one ProxLink for your Central Console computer. The serial number (located on a silver tag on the bottom of the ProxLink) of this ProxLink must be entered in the **Destination Serial Number** and **Serial # Filter** location on all ProxLink Radios connected to the transponders.

1. Attach the PC to the ProxLink using the ProxLink RS-232 cable. Attach the DB-9 Connector to the ProxLink and attach the DB-25 female connector the PC. Gender changers or DB-25 to DB-9 converters may be required depending on your serial port connector type.
2. Start your terminal emulation software (Hyper Terminal). Configure the ProxLink as follows: 9600 Baud, 8 Data Bits, 1 Stop Bit, and no parity.
3. Put the ProxLink in User Interface Mode by pressing the **[CONFIGURATION]** button on the front of the unit. The ProxLink should respond by displaying the **Main Menu** screen.
4. Once the **Main Menu** is displayed, configure a ProxLink parameter by selecting a menu option and pressing the <Enter> key. This will either display a prompt or a sub-menu. After finishing with a sub-menu, press the <Esc> key to return to the previous menu.
5. After you have finished configuring the ProxLink, type <L> <Enter>, then type <Y> to place the unit in operating mode.

Configuration should look as follows in Main Menu, D - Display ProxLink Radio Module Parameters:

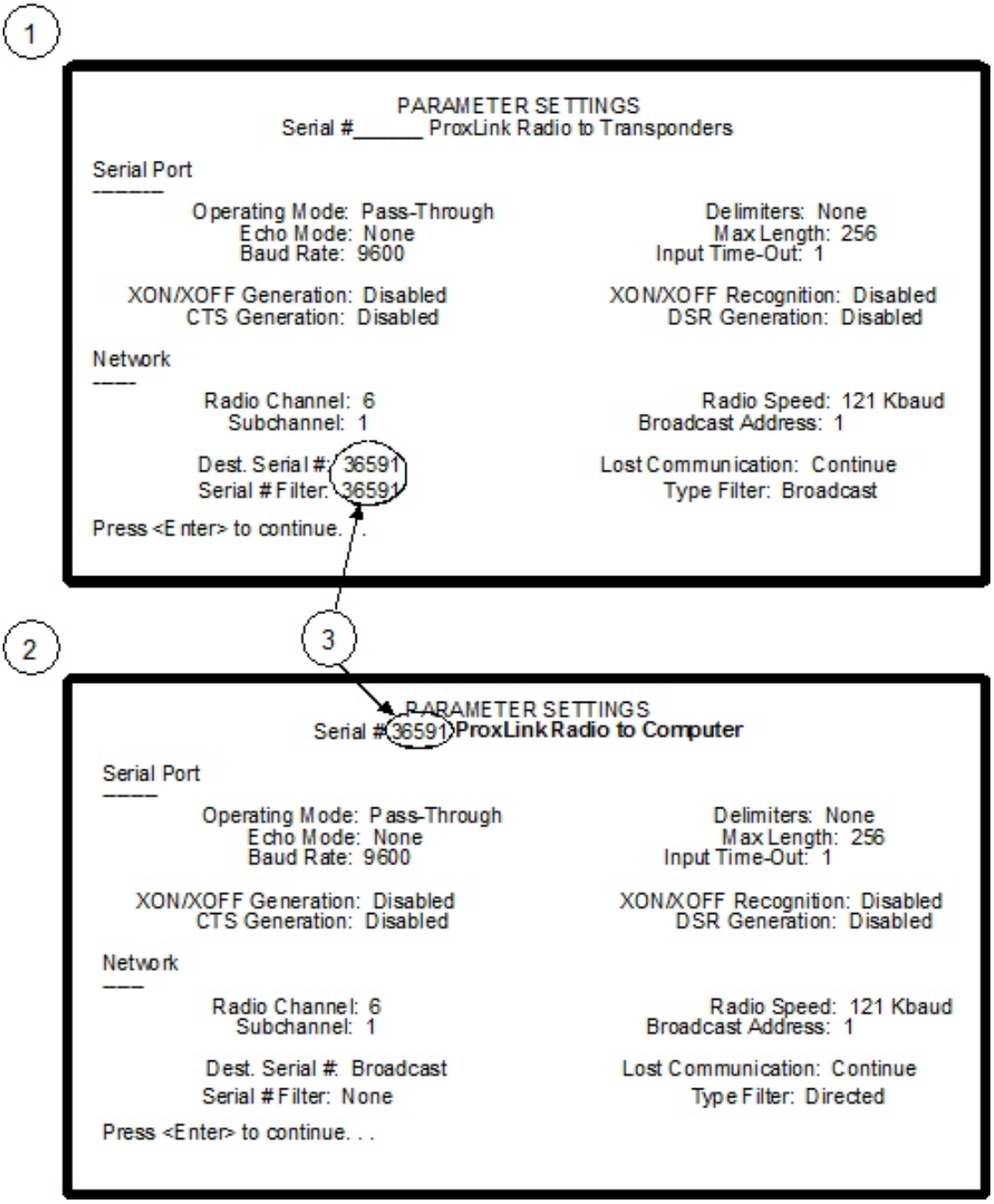


Figure 4.17: ProxLink Radio Module Configuration

1	ProxLink radio module configuration for the transponders	3	These numbers must match
2	ProxLink radio module configuration for the central station		

5 System power-up and debug

5.1 Initial system configuration

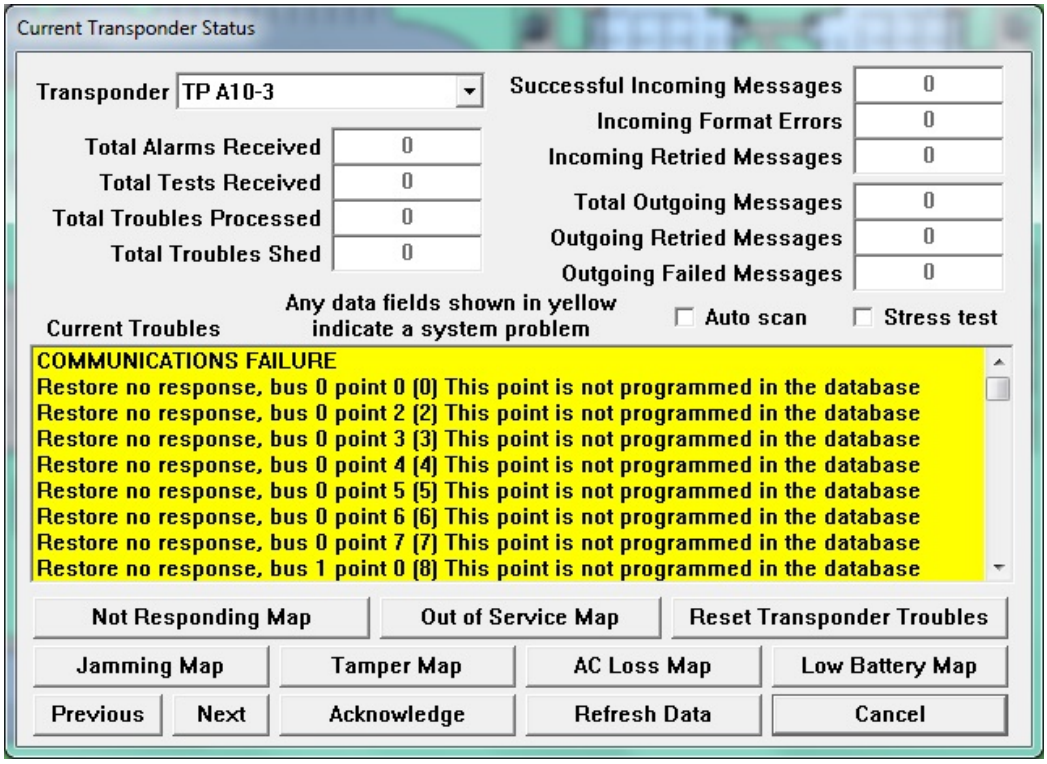
Refer to the section *Initial System Configuration* in the Security Escort *Technical Reference Manual* document to configure the software. Transfer the information from the installation data sheets to the **Transponder Database** and assign the communication ports to the SE485 bus or ProxLink Radio. Make sure that the databases are backed-up using the menu **Utilities > Backup** selection. Back-up the databases whenever they change, and keep multiple copies.

5.2 Powering up the system for the first time

After the system is configured, the system may be powered up. If the system uses multiple transponders, it is easier and more effective to power up the transponders one at a time. By doing this, troubleshooting time can be significantly reduced, especially for transponders to determine if there is a wiring problem in the SE485 bus between transponders.

Notice!
It is very important that twisted pair wiring is used for the SE485 bus. The Tx+ and Tx- wires must be twisted together and the Rx+ and Rx- wires must be twisted together.

1. Turn on the power switch on the first transponder. In the Security Escort Central Console software, select the menu **Setup > Transponder current status**. The following dialog window appears:



2. Select the desired transponder. Click the **[Reset Transponder Troubles]** button. If the selected transponder is communicating with the Central Console, the number “1” will appear in the **Total Outgoing Messages** and **Successful Incoming Messages** fields. The

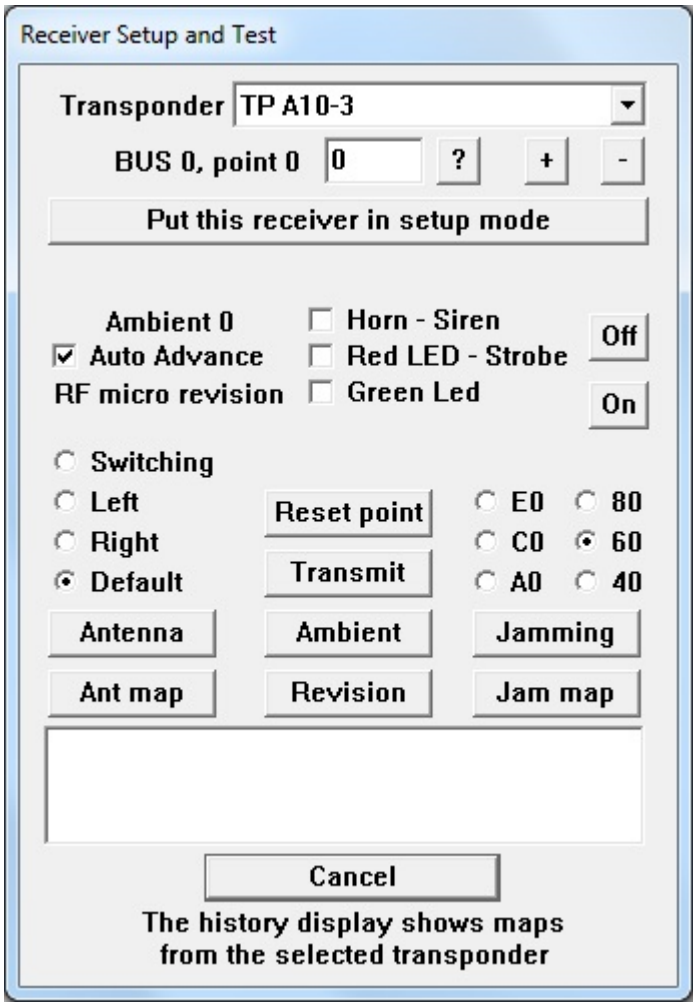
transponder is now communicating with the Central Console software. If the number “1” only appeared in the **Total Outgoing Messages** field, there is a wiring problem between the Central Console and the transponder (refer to Troubleshooting reference of this manual and locate the problem).

3. Check the **Stress test** checkbox. This tests the communications reliability by causing the Central Console software to send a continuous stream of messages to the selected transponder. The values in the **Successful Incoming Messages** and **Total Outgoing Messages** fields should start counting up rapidly, with few if any errors. It is normal to have slightly fewer **Total Outgoing Messages** than **Successful Incoming Messages**. If the errors are greater than 1% of the number of messages, then there is a problem that should be corrected (refer to Troubleshooting transponders, points, receivers, and alert units of this manual and locate the problem).

4. After the stress test runs, any current troubles are displayed in the box in the **Transponder current status** window. Correct any troubles at this time.

5. When the transponder is communicating with all the receivers and the **Receivers Database** records are correct, back up the database files to the hard drive, if any changes were made. Select the menu **Utilities > Backup**, and make sure it is pointed to the hard drive. Click the **[Backup]** button. It is also wise to back up each database to a USB flash drive. Mark the USB flash drive label with the databases and backup date.

6. To confirm the RF reception, LED and sounder operation, and location of each receiver, select the menu **Setup > Receiver configuration**. The following dialog window appears:



7. Select the desired transponder.
   - Click the **[?]** button next to the **point number** field. A grid of bus and point numbers appears showing the programmed receivers.
   - Click the lowest point number button. If the first receiver is point zero (0), click the **[0]** button. If the first receiver is point one (1), click the **[1]** button. The point number is automatically entered.
   - Click the **[Put this receiver in setup mode]** button. The red and green LED light up for the selected receiver on the selected transponder.
   - Take the maintenance transmitter and go to the selected receiver. The red and green LED should be lit when you arrive at the first receiver location.
   - Transmit an alarm from the maintenance transmitter. The receiver should activate by flashing the red LED and activate the sounder (if the sounder jumper is in place on the receiver). This confirms that the RF portion of the receiver is working and you are at the right location. The software then turns off the LEDs on the tested receiver. The receiver with the next higher point number is automatically selected and its red and green LED lights up.

– Proceed to that receiver and perform the same operation with an alarm on the maintenance transmitter until the operation of all receivers is confirmed and all receivers are working and in their proper location on that transponder. If the LED fails to light up, the LED jumpers may be missing on that receiver, the receiver may be set to the wrong address, or you may be at the wrong location. If the LED are lit but the receiver fails to respond to the maintenance alarm, there may be a problem with the receiver board or another receiver is receiving a stronger signal.

8. Repeat the sequence above starting with step 1 for all transponders and receivers in the system.

6 Testing and troubleshooting

6.1 Built-in troubleshooting aids

Notice!
Refer to *Troubleshooting reference, page 59* for wiring troubleshooting where applicable.

6.1.1 EA102 receiver

Jumpers
There are two groups of jumpers on the EA102A-304 receiver. The first group contains jumpers P1 through P3. The second contains jumpers P4 through P8. The function of each jumper is indicated in the table below:

Jumper	Operation with Jumper in Place
P1*	Sounder is enabled
P2*	Green LED is enabled
P3*	Red LED is enabled
P4**	Test mode is enabled
P5**	Receiver spacing mode is enabled
P6**	Left antenna is disabled
P7**	Right antenna is disabled
P8	Do not place a jumper across these pins

Notice!
* Remove jumpers P1, P2, and P3 when installed in an outdoor enclosure.
** Remove jumpers P4, P5, P6, and P7 for normal operation.

Test mode
Each EA102A receiver provides a test mode that may be used to check the unit's functionality. The module goes into test mode when jumper P4 is in place (jumper P5 removed). In this mode, all test and alarm receptions will be sounded.

Notice!
The sounder and LEDs (jumpers P1, P2, and P3) must also be enabled to operate the test mode.

Each receiver should be tested using the following method (test only one receiver at a time):

1. Enable the test mode by placing the jumper P4 across both pins (jumper P5 removed).
   - The red LED will turn ON and stay ON during the test. This indicates that power is properly connected and the receiver is in test mode. If the red LED does not come on check the POWER+ and POWER- wiring to this receiver. Also verify the corresponding transponder bus enable jumper is in place and the transponder is on and powered.
   - The green LED will flicker if the receiver is connected to a working transponder. If the green LED is not flickering verify the BUS+ and BUS – wiring to this receiver (note, this is a rapid flickering).
   - There will be no data transmitted to the Central Console. Therefore, the Central Console will report this receiver as “Not responding” while the receiver is in test mode.
2. Activate the transmitter from different locations near the receiver.
   - The red and green LEDs will respond to a received transmission.
   - If the receiver detected all the packets from the transmission, the sounder will beep three times.
   - If the receiver detected the transmission, but some of the packets were missing, it will beep once. This could indicate that the signal is not sufficient from this location.
3. Remove the jumper P4 to return the receiver to normal operating mode.

Receiver spacing mode

Refer to *Verify each potential receiver location, page 21* to determine receiver location and spacing.

6.1.2 EA500 transponder

Status LEDs

Each transponder contains LEDs that display the transponder’s condition and its response to events. With the exception of the AC Power LED (which is located in the lower right corner of the transponder circuit board), the diagnostic LEDs are located in the top right corner of the transponder board.

Generally, the LEDs indicate the unit’s status and signal system events. Each LED and its function is indicated below.

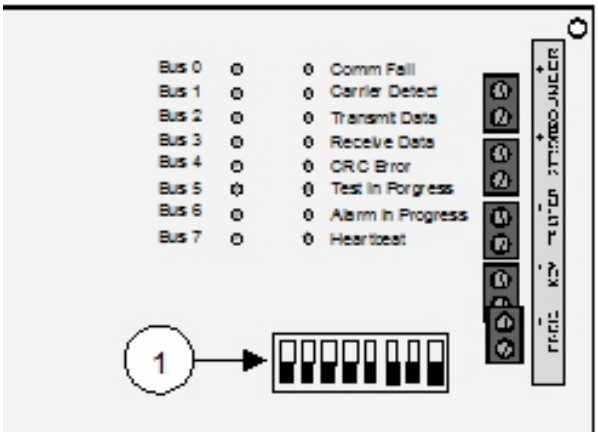


Figure 6.1: EA500 Diagnostic LEDs

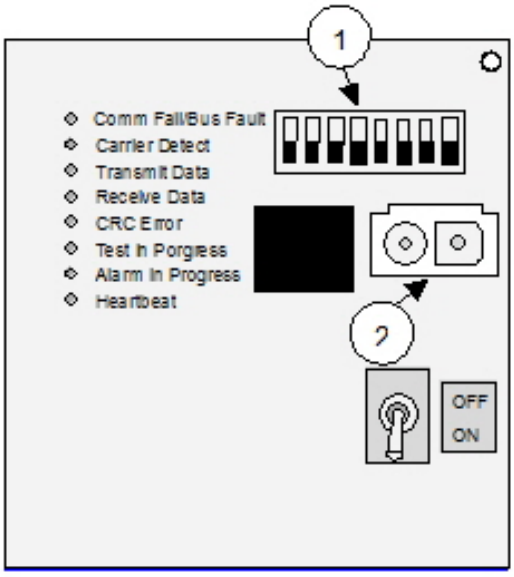


Figure 6.2: EA501 Diagnostics LEDs

LED	Function
AC Power	(Lower right corner of the transponder board.) If this LED is off there is no AC power (mains power) to the board. Find and correct the AC power (mains power) problem. This LED lights even if the transponder's power switch is off.
Comm Fail	This LED lights if the transponder is in a communications failure condition with the Central Console. It automatically goes out when communications are restored.
Carrier Detect	This LED is operational only for SE485 communications. It flashes every time any transponder (including this transponder) on this SE485 bus sends a message to the Central Console. It is used to monitor overall communications from the transponders to the Central Console. If the Carrier Detect LED stays on, there is a problem with one of the transponders on this bus, or the wiring, that must be corrected before normal communications are restored.
Transmit Data	This LED flashes every time this transponder sends a message to the Central Console, whether or not the Central Console receives it. If this transponder initiated the communications and the Central Console correctly receives the message, the Receive Data LED should flash soon after indicating the central station successfully returned an acknowledgement.
Receive Data	This LED flashes every time this transponder successfully receives a message addressed to it from the Central Console. If the Central Console initiated the communications, the Transmit Data LED should flash soon after indicating that this transponder is returning an acknowledgement.

LED	Function
CRC Error	This LED comes on every time a message is received containing errors, whether or not it was addressed to this transponder. The LED remains on until the next message addressed to this transponder is received without error. The most common cause for this LED to turn on is wiring errors. Verify that the SE485 TX+ and TX- are on a twisted pair. Also verify that the SE485 RX+ and RX - are on a twisted pair.
Test in Progress	This LED comes on whenever a transmitter is tested. It stays on for the duration of the test display, typically 5-sec. to 10-sec., then it goes out. If a test is received while another test is in progress, the Test in Progress LED goes out momentarily then comes on for the duration of the second test.
Alarm in Progress	This LED comes on whenever a transmitter is in alarm. It stays on for the duration of the transponder's involvement in the alarm, then it goes out. If an alarm is received while another alarm is in progress, the Alarm in Progress LED goes out momentarily then stays on as long as any alarms are active in the transponder. An alarm that causes the receiver sounders to stay on keeps the Alarm in Progress LED on. Silent alarms or alarms from unauthorized transmitters cause the Alarm in Progress LED to turn on and to go out when the Central Console acknowledges the alarm message. This also occurs for every alarm follower message. A maintenance alarm message causes the Alarm in Progress LED to come on for 5-sec. to 10-sec. then to automatically go off.
Heartbeat	Flashes at a fixed rate to indicate the microprocessor is operating normally. If this LED stops flashing, the transponder is not operational. Turn it off for 5-sec. using the power switch. Then turn it back on. If the LED does not flash, the transponder should have the AC power and the back-up battery disconnected. Wait a few seconds and then reconnect. If the LED does not flash at this time, the transponder should be replaced.
Bus 0 to 7	Normally these LEDs are on if the corresponding Bus Enable jumper is in place, and is off if the jumper is removed. If the bus is enabled, the LED flashes off and comes back on every time a receiver or alert module on that bus communicates with the transponder. A Bus LED flashes at the rate of the heartbeat LED if there is any kind of bus fault (data to ground, data to power, and bus power to ground) on that bus. On the EA501, the communications failure LED flashes at this rate since there is no Bus LED. A Bus LED flashes at half the rate of the Heartbeat LED if there are no points reporting on that bus (open connection). On the EA501 the communications failure LED flashes at this rate. If a Bus LED is flashing for a bus that is not enabled, it can be reset in the Central Console's **Transponder Data View** dialog by selecting this transponder and clicking the **[Clear EE]** button. There are two special displays on the Bus LEDs. All the Bus LEDs go out, and for 2-sec. a single LED is on. Walking down the

LED	Function
	display from bus 0 to bus 7 indicates that a battery test is in progress. Usually after the tamper switch is released, the bus LEDs count rapidly to indicate the EEPROM memory is being updated.

Verifying communications

To verify communications, press the test feature on any transmitter. The Test in Progress LED comes on. If it did not come on, the receivers are not communicating with the transponder. About a second after the Test in Progress LED comes on, the Transmit Data LED flashes (indicating the transponder is sending the test message to the Central Console). Less than a second later the Receive Data LED flashes (indicating the Central Console returned an acknowledgement).

Toggling the transponder's tamper switch on/off causes the Transmit Data LED to flash (indicating that the transponder is sending the tamper message to the Central Console). Less than a second later the Receive Data LED flashes (indicating the Central Console returns an acknowledgement).

6.2 Troubleshooting reference

Symptoms	Probable Cause	Possible Solutions
All transponders on one bus in communications failure	Power to SE485.	Check 9 V DC adapter for proper voltage. Red Power LED should be ON (on SE485).
	Wire between SE485 and transponder incorrectly installed.	Check to make sure transmit from transponder goes to receive of SE485 and receive from transponder goes to transmit on SE485 (RX+ to TX +, RX- to TX-).
	Open, short, or grounded cable from SE485 to first splice or transponder.	Use VOM to test cable for short, open or ground. Repair or replace cable. Also check for + - pair reversed.
	Wrong cable between SE485 and computer.	Cable should be a straight through cable to your computer serial port connection. Do not use null modem cable or cable marked for printer.
	Bad SE485 Module.	Replace SE485 Module.
	Using third party RS-485 interface.	Due to changes made for transient protection, transformer isolation, and link busy detection, these signals are not compatible with third party RS-485 Interfaces. Replace with SE485
High communications error count.	Wire between SE485 and transponder incorrectly installed.	Check to make sure transmit from transponder goes to receive of SE485 and receive from transponder goes to transmit on SE485 (RX+ to TX +, RX- to TX-).
	Wrong wire type.	Wire type must be twisted pair.
Single transponder in communication failure.	Transponder not on.	Check power switch.
	Wrong transponder address.	Check DIP switch setting on transponder to correspond with your transponder data base setting.

Symptoms	Probable Cause	Possible Solutions
	RS-232/SE485 switch position.	Check slide switch on transponder to make sure it is in the SE485 position.
	SE485 wiring on transponder.	Check to make sure transmit from transponder goes to receive of SE485 and receive from transponder goes to transmit on SE485 (RX+ to TX +, RX- to TX-).
	Close lightning hit.	Power down transponder and restart. If this does not work replace transponder.
	Bad transponder.	Replace transponder.

Tab. 6.7: Transponder communications with SE485 bus

Symptoms	Probable Cause	Possible Solutions
Communication failures from all transponders.	Loss of power.	Check power to ProxLink from Central Console. Also, if using SE485, check power to SE485 module.
	Cable from ProxLink to computer.	Must use 25 to 9 pin cable supplied from Proxim.
	ProxLink Radio Module might be in Programming Mode.	Unplug power to ProxLink and plug back in to re-start ProxLink.
	SE485 Module.	Check wiring between SE485 and computer, and SE485 at ProxLink Radio Module. Transmit should be going to receive and receive should be going to transmit (RX+ to TX+, RX- to TX-).
	Cable from SE485.	Cable from SE485 to computer must be straight through 25 pin to 25 pin or 25 pin to 9 pin depending on your serial port on the back of the computer. Do not use cable labeled for printer or null modem cable. Replace cable if bad. Check cable between SE485 and ProxLink Radio Module. Replace if bad.
	ProxLink Radio Module.	Check programming for Central Console ProxLink Radio Module to be sure it is correct. If everything else checks OK, replace ProxLink..
One transponder in communication fail on ProxLink Radio Module link.	Transponder.	1. Check slide switch on transponder to make sure it is in the RS-232 position. 2. Check DIP switch address for transponder to be sure it corresponds with **Transponder Database**.
	Cable from ProxLink Radio Module to transponder.	Replace cable.

Symptoms	Probable Cause	Possible Solutions
	ProxLink Radio Module.	3. Check power to ProxLink. Make sure radio power LED is lit. 4. Check antenna connection to ProxLink Radio Module. 5. Check programming for ProxLink Radio Module. 6. Radio out of range or not in line of sight of central console antenna. 7. Ice on antenna. 8. If antenna is remote from ProxLink, use RG8U cable to prevent dB loss. 9. Replace ProxLink Radio Module.
	SE485.	10. Check power to ProxLink to SE485. 11. Make sure slide switch on transponder is set for SE485. 12. Check wiring from transponder to SE485 (RX+ to TX+, RX- to TX-). Make sure transmit goes to receive and receive goes to transmit. 13. Replace SE485 Module.

Tab. 6.8: Transponder communication with ProxLink

Symptoms	Probable Cause	Possible Solutions
Bus failure.	Bus power jumper not in place.	Place jumper on for corresponding bus (see the transponder's *Installation Instructions* for location of jumper).
	Short or open on the bus wires.	Put meter across bus wire. Should be reading between 7.5 V DC to 10.5 V DC. If voltage is not present or lower than 9 V, check wiring (BUS+ to BUS-) for possible ground, short, or open.
	No power to receiver.	Check power for 10.5 V DC to 13.5 V DC. If lower than 10 V DC or no voltage present, check wiring (PWR+ to PWR-) on power side of receiver, repair, or replace cable.
	Close lightning hit.	Power down transponder (AC and battery) for 30-sec., then turn power back on. If bus failure does not clear, probable cause would be bad bus on transponder.
	Bad bus on transponder.	Remove cable from bus, meter terminals with VOM. If voltage is lower then 9 V DC on BUS+ or lower then 12 V DC on PWR+, replace transponder.

Tab. 6.9: EA500 transponder bus faults

Symptoms	Probable Cause	Possible Solutions
Single receiver not responding.	Address switch in wrong position.	Rotate switch to correspond with transponder database location.
	Open on the bus wires.	Put meter across bus wire. Should be reading between 7.5 V DC to 10.5 V DC. If voltage is not present or lower than 9 V, check wiring (BUS+ to BUS-) for possible ground or open.
	No power to receiver.	Check power for 10.5 V DC to 13.5 V DC. If lower than 10 V or no voltage present, check wiring (PWR+ to PWR-) on power side of receiver repair or replace cable.
	Defective receiver.	If power is present on BUS+ and PWR+ and rotary switch is set to correct address, replace receiver.
Single receiver intermittently not responding.	Receiver is located past the 900 m (3000 ft) maximum cable run.	Re-engineer location or reroute cable to be under 900 m (3000 ft).
	Moisture on circuit board.	Seal housing where moisture is entering enclosure. Replace receiver until the old one dries out.
	Cable going to ground occasionally.	Replace or repair cable.
	Insects nesting on circuit board.	Seal any entry point and spray insect repellent inside housing to stop any further invasions into receiver.
	Bad splice to receiver.	Check all splices to make sure cables are tight and not loose causing high resistant open.
	Defective receiver.	If power is present on BUS+ and PWR+, between 7.5 V DC and 10.5 V DC on bus, and 10.5 V DC and 13.5 V DC on power, replace receiver.

Symptoms	Probable Cause	Possible Solutions
Single receiver reporting bad check sum.	Two receivers on the bus with the same address ID number.	Check rotary switches on all receivers on that bus to be sure there are no duplicate ID numbers.
	Moisture or water on receiver.	Replace receiver with new one until the old receiver dries out. Seal any point where moisture is entering the receiver housing.
	Length of cable to receiver. Receiver is mounted over 900 m (3000 ft.) from transponder.	Reconfigure the bus run to make sure receiver is within 900 m (3000 ft.) of the transponder.
	Bad splice to receiver.	Check all splices to make sure cables are tight and not loose causing high resistance open.
	Defective receiver.	If power is present on BUS+ and PWR+, between 7.5 VDC and 10.5 VDC on bus and 10.5 VDC and 13.5 VDC on power replace receiver.
Receiver jamming.	Electrical equipment in area causing jamming on receiver.	Go to the software dialog **Setup** r**eceiver configuration**. Increase jamming threshold by one degree at a time until jamming stops and receiver returns to normal. If jamming persists after increasing level, relocate receiver or attempt to identify and minimize the jamming source.
Receiver LEDs not working.	LEDs not positioned behind viewing lens.	Remove cover, straighten LEDs, replace cover carefully so LEDs are positioned behind viewing lens. Use maintenance transmitter on test and alarm after installing cover to check visibility of LED.
	Jumpers in “OFF” position on receiver.	Remove cover, check jumpers to right of sounder above red LED and make sure jumpers P2 and P3 are “ON”.

Symptoms	Probable Cause	Possible Solutions
	Bad receiver.	After performing the steps above and LEDs still do not operate on test or alarm, replace the receiver.
Receiver's sounder not operating.	Jumper in "OFF" position on receiver.	Remove the cover, check jumper to right of sounder above red LED and make sure jumper P1 is "ON".
	"Run Silent" is turned on in the Central Console software.	At the Central Console, select menu **Setup** > **Transponder Parameter** dialog and un-check the **Run Silent** checkbox.
	Bad receiver.	If the sounder still does not operate after performing the steps above, replace the receiver.

Tab. 6.10: EA102 receiver issues

Symptoms	Probable Cause	Possible Solutions
Communication failures from all transponders.	Loss of power.	Check power to Moxa/ Lantronix device.
	Cable from Moxa device to transponder.	Must use standard 9 pin female to 9 pin male cable.
	Cable from Lantronix device to transponder.	Must use modified 25 pin male to 9 pin male cable. Refer to the Lantronix wiring notes.
	Moxa/Lantronix device might not be running.	Unplug power to Moxa/ Lantronix device and plug back in to restart Moxa/ Lantronix device.
	Cable from Moxa/Lantronix device to Ethernet network.	Check Ethernet cable between Moxa/Lantronix device and Ethernet network. Replace if cable is bad.

Tab. 6.11: Transponder communication with Moxa/Lantronix device

6.3 Software Troubleshooting

Security Escort uses two network connections between the master computer and the slave computer and workstations.
The retrieve database access to all the Security Escort databases is through the Micro Kernel Database Engine (MKDE). The MKDE on each computer automatically opens a connection to the master databases. The path to the master databases is defined under the **Network** menu in the **System Directories and Network Address** dialog as the **Master Database Path** textbox.
The second connection is through a TCP/IP socket that the slave computer or workstation opens to the master. The IP address and port to the master computer is defined under the **Network** menu in the **System Directories and Network Address** dialog as the **Master's Network Address** textbox and the **Master's Network Listen Port** textbox. There is also a similar address and port for the slave computer.
Stored with the master database path is the global preference file (gprefers.edb). The Security Escort application on the master computer must be run first. Under the **Network** menu in the **System Directories and Network Address** dialog, click the **[Learn Address]** button. This automatically fills in the **Master's Network Address** and the **Master's Network Listen Port** textboxes". Save the change. This places the master's network address and port in the global preferences file.
When the slave and workstation computers are first started, set the path to the master database under the **Network** menu in the **System Directories and Network Address** dialog as the **Master Database Path** textbox. When the path is set, shut down the Security Escort application without making any other changes and restart it. The slave or workstation computer then reads the software key information and the master's network address and port from the global preferences file. This allows the **Operator Database** to open successfully and the network connection to open to the master computer.

6.3.1 "CAN'T OPEN THE OPERATOR.EDB FILE" error

If a yellow box is displayed with the message "Can't open the OPERATOR.EDB file," the file might be missing or corrupt, the software key or its driver might not be installed, or the database manager might not be loaded. To correct, use the Restore or Install buttons. If the slave computer cannot open the Operator database, check the following:

- Verify the master computer can access the databases by starting Security Escort first. Also verify the Security Escort software does not indicate it is running in "Demo" mode.
- Verify the correct type (default master computer, default slave computer or workstation computer) is set in the **Remote Setup** dialog under the **Setup** menu. There can be only one master computer and one slave computer in a system. Only the master computer has a software key installed.
- Check to see if the master database path is set up correctly in the **System directories and Network Address** dialog under the **Network** menu on both the slave and workstation computers. Confirm the drive letter used is the correct letter that was set up in the Map Network drive. You might have to double click the Security Escort icon and immediately press and hold down the <Ctrl>, <Shift>, and <Tab> keys on the keyboard. Do not release the keys until the **System directories and Network Address** dialog displays. Make any changes required and click the **[Save]** button. Repeat through all of the setup screens.
- Determine if the slave computer can access the shared drive on the master computer. We verified this access in the Map the master's network drive from each slave and workstation for the slave computer when we read the readme.txt file. Re-verify this connection and that you can read and write files (edit the readme.txt file remotely to test the ability to write).
- Determine if the slave computer can access the global preferences file (gprefers.edb) that is stored in the same directory as the OPERATOR.EDB file on the master computer.
- Determine if the master computer saved the global preferences correctly. Verify the preference settings on the master computer. Even if they appear correct, change something in the System directories and network address dialog on the master computer and click the Save button. This forces the global preferences to be rewritten. Now change the setting back to where it should be and click the Save button again.
- Verify the TCP/IP settings in the network control panel are correct.

6.3.2 Network connection fails

If the databases can be accessed and the Security Escort program starts up but indicates that a network connection failed:

- Check that the master and slave (if used) computers have a static IP address. The workstations can have dynamic IP addresses.
- Check to see if the **Master's Network Address** and **Master's Network Listen Port** fields are saved correctly in the **System directories and Network Address** dialog under the **Network** menu on the slave and workstation computers. Verify these preference settings on the master computer. Even if they appear correct, change something in the **System directories and network address** dialog on the master computer and click the **[Save]** button. This forces the global preferences to be rewritten. Now change the setting back to where it should be and click the **[Save]** button again.
- Stop and start the Security Escort program on the master computer. Then stop and start the Security Escort program on the slave computer.
- Confirm the **Slave's Network Address** and **Slave's Network Listen Port** fields are saved correctly in the **System directories and network address** dialog under the **Network** menu on the workstation computers.

- Try changing the **Master's Network Listen Port** number and click the **[Save]** button. If you do change the port number, exit the Security Escort program on the master computer and then restart it. Then restart the slave computers. Try port numbers in this order 4561, 5001, 6001, 7001, 8001, and so on.
- If the master and slave computers are on different LAN or WAN segments, verify the gateway setting in the TCP/IP section of the network control panel is correct.
- Verify the TCP/IP settings in the network control panel are correct. Database edits can be made from any computer and all computers instantly see the changes. If another computer has a database record open in the editor and another computer attempts to edit that record, the record is locked, a message pops-up, and you cannot edit the record from the second computer. Another computer cannot edit that record even after the first computer saved the record, until the first computer edits another record.

6.3.3 "THE MASTER COMPUTER MUST BE ON-LINE TO RETURN THE SYSTEM TO OPERATIONAL STATUS" message

This may be normal.

The system is designed to allow the slave and workstation computers to operate for about a week if the master computer fails. To accomplish this, the master computer writes specific data to the global preferences file each evening that is based on the software key and the time and date. The slave and workstation computers then read this data to determine if they are allowed to run a system. Until the master computer has run continuously over night with a valid software key attached, these specific values are not in the global preferences file. Therefore the "THE MASTER COMPUTER MUST BE ON-LINE TO RETURN THE SYSTEM TO OPERATIONAL STATUS" message is displayed. Once the master computer has run overnight, this message disappears. If the master computer fails, has its software key removed, or is taken off-line, the "The slave computer has xxx hours of operation left before an operational master must be online" message appears. This happens when there is approximately four days of operation left.

7 Appendix: Information sheet and files required

7.1 Transponder information sheet

Transponder Number:		**Transponder Location:**	
Transformer for Transponder Location:			
Breaker Panel Location:		**Breaker Number:**	
Siren/Strobe Output To:			
Keyswitch Monitoring To:			
Bus #0 Locations:			
Point #0:			
Point #1:			
Point #2:			
Point #3:			
Point #4:			
Point #5:			
Point #6:			
Point #7:			
Bus #1 Locations:			
Point #0:			
Point #1:			
Point #2:			
Point #3:			
Point #4:			
Point #5:			
Point #6:			
Point #7:			
Bus #2 Locations:			

Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #3 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #4 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #5 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	

Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #6 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Bus #7 Locations:	
Point #0:	
Point #1:	
Point #2:	
Point #3:	
Point #4:	
Point #5:	
Point #6:	
Point #7:	
Location of Splices:	

7.2 Files required for Security Escort

The following files must be in the same directory as ESC32.EXE (default “C:\ESCORT”).

Files	Description
Esc32.exe	the main program
Bwcc32.dll	support for the dialog appearance
Cdrvdl32.dll	communications support
Cdrvhf32.dll	communications support
Cdrvxf32.dll	communications support
Commsc32.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

The following files are the preferences for this workstation and are stored in the same directory as ESC32.EXE.

Files	Description
Wprefers.edb	the workstation preferences settings
Prefersc.edb	Old system preferences settings. This file is converted to gprefers.edb and wprefers.edb, and then is automatically deleted.

The map of the facility is a standard Windows bitmap (BMP) file. It must be stored in the same directory as ESC32.EXE.

Files	Description
MAP0.EDB	Main map bitmap file.
MAP1.EDB	Extra map bitmap file if used.
MAP2.EDB	Extra map bitmap file if used.

The following files are the system databases that are stored at the Master Database path (duplicate copy in the Slave Database Path).

Files	Description
Operator.edb	System Operators Database

Files	Description
Preferen.edb	System Preferences settings
Reports.edb	Alarm Reports database
Subscrib.edb	Database of the Subscribers/ Transmitters
Transpon.edb	Database of the System Configuration
Gprefers.edb	Global system preferences settingss

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

Files	Description
SEtroubl.wav	trouble sound
SEalarm.wav	alarm sound

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”)

Files	Description
Image1.jpg	sample subscriber image
Image2.jpg	sample subscriber image
Image3.jpg	sample subscriber image

Index

A

AE 101 Enclosure
- Specifications 17

AE1 Enclosure
- Description 16
- Specifications 16

AE100 Enclosure
- Description 17
- Specifications 17

AE101 Enclosure
- Description 17

AE3 Enclosure
- Description 16
- Specifications 16

Alert unit
- address 48
- estimating number of 21
- mounting 47
- wiring 35, 48

B

Batteries 16

C

Cables 14

Central Console
- Function of 8
- initial system configuration 51
- minimum system requirements 9
- software overview 8
- versions 9
- wiring 35, 38, 41

Compatible parts 8

Components
- mounting and setting up 45

Computer to SE485 cable
- description 16
- specifications 16

E

E28629B Battery
- Description 16
- Specifications 16

EA102 receiver
- address 45
- description 10
- mounting 45
- specifications 11

EA120 alert unit
- description 11
- specifications 11

EA500 transponder
- description 10
- specifications 10

Enclosures
- mounting 45

Equipment estimation
- general 19

F

Files required 73

I

Indoor receiver installation 22

Installation process 29

L

Lantronix interface
- DB25 pinouts 38
- wiring 38

Lantronix interface adapter
- description 11
- specifications 12

Lantronix to transponder cable
- description 15
- specifications 15

Location accuracy 18, 21, 24, 26

M

Master to slave
- specifications 15

Master to slave cable
- description 15

Minimum system requirements 9
Moxa interface
DB9 pinouts 36
wiring 35
Moxa interface adapter
description 11
specifications 11
Moxa to transponder cable
description 15
specifications 15
Moxa/Lantronix
troubleshooting 68

N

National Electrical Code 30

O

Outdoor receiver installation 23

P

Personal Escort transmitters 12
Pre-construction coverage verification survey 21
ProxLink
configuration 49
setup 49
troubleshooting 62

R

Receiver
determining receiver location 21
installation 22, 23
mounting 45
spacing 56
testing receiver spacing 21
troubleshooting 65
Receivers
estimating number of 19

S

SE2 personal transmitter
description 13
specifications 13
SE3 subscriber transmitter family
description 14
specifications 14
SE3401 point tracking transmitter
description 14
specifications 14
SE485 interface
wiring 41
SE485 interface adapter
description 12
specifications 12
troubleshooting 60
Siren Strobe 17
Site Survey 21
General 18
System block diagram 7
System power up 51
System power-up 51

T

Transponder
address 45
estimating number of 20
mounting 45
system power up 51
troubleshooting 60, 62, 64, 68
wiring 35, 45
Troubleshooting 55
aids 55
Reference 59

W

Wiring
alert unit 35, 48
EA500 transponder 45
general 29
Lantronix 38
Moxa 35
receiver 35
SE485 30, 41
transponder 35

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com
© Bosch Security Systems B.V., 2019