Actall Corporation

ISO 9001:2015 Certified

PALS 9K | Installation Manual

Version 4.0

COPYRIGHT & LIMITATIONS

Software License Agreement:
The use of this software product is limited to the terms and conditions below. Use by the purchaser of Crisis Controller©™ Alarm Monitoring software indicates acceptance of these terms.

Grant of Rights:
This software may only be used on the computers for which it is licensed. This license may not be transferred from its original site. You may not copy or otherwise distribute this software, except to make a backup copy. You may not modify, alter, or transfer the software in any way.

Limitation of Liability:
Licensor shall not be liable for any claim or demand by Licensee for damages of any kind, including, but not limited to special, general, incidental, direct or consequential dam-ages, for loss of business profits, business interruption, loss of business information, or any other pecuniary loss arising out of the subject matter of this agreement Some jurisdictions do not allow excluding or limiting implied warranties or limiting liability or consequential damages, and some jurisdictions have special statutory consumer protection provisions that may supersede this limitation. As a result, this limitation of liability may not apply to you if prohibited by the laws of your jurisdiction.

General:
Any violation of this Agreement is subject to criminal and civil prosecution. If any provision is found to be unlawful, void, or unenforceable, then that provision shall be severed from this Agreement and will not affect the validity and enforceability of any of the remaining provisions. The laws of the State of Colorado shall govern this Agreement.

CONTACT

Inquiries should be directed to:

Actall Corporation
2017 Curtis Street
Denver, CO 80205

Phone:
303-226-4799
Toll-free:
1-800-598-1745

For technical support, please call us direct during regular business hours (Monday through Friday, 8:00 a.m. to 5:00 p.m. Mountain Standard Time) or Emai us 24/7.

303-226-4799
support@actall.com

Table of Contents

Crisis Controller©™ Monitoring Center

The Crisis Controller©™ Alert Monitoring Center receives and supervises alarm information from wireless security devices and transmitters. Data from these devices is processed by the software and displayed to rapid response to alarms and trouble conditions.

Equipment

The PALS©® Alert Monitoring Center consists of a central monitoring computer, which receives data from wireless 900MHz transmitters through a serial receiver. Numerous types of transmitters are available, including fixed-position contact sensors, motion and smoke detectors, and personal alarm transmitters. The software can also process signals from Actall Security Product's® Personal Alarm Locating System (PALS©®), which transmits location data from fixed position infrared (IR) Locators to The transmitters then communicate their location to the Monitoring Station, allowing Control Operators to track and locate positions of the individuals wearing the mobile alarm devices.

How Transmitters Communicate with Receivers

Wireless transmitters send coded digital messages to the serial receiver(s). These messages contain data identifying the transmitter and its status. Multiple transmissions of this data over the 902 to 928 MHz frequency range help prevent signal interference and ensure that the signal is received.

Serial Receiver

Serial Receiver(s) identify valid messages, decodes them, and transmits that data to the Crisis Controller©™ software for alarm annunciation on the Alarm Monitoring PC.

Most sites require the use of wireless repeaters: 900MHz transceivers (powered by 14VAC) that identify valid transmissions and re-transmit them at full signal strength. Repeaters provide a method of extending effective transmission ranges and of providing multiple, redundant transmission paths between transmitters and receivers.

Serial Receiver

The Personal Mobile Transmitters (PMTs) used with the PALS©® systems work in conjunction with IRT Locators to provide detailed information of location and movement. PMTs store the two most recently received IRT Locator codes. When an alarm is sent, this data is sent along with the alarm status to a serial receiver attached to the Monitoring Center PC. If a PMT remains within the coverage area of the same Locator for a longer period of time, the programmer can increase the time interval between PMT readings. This reduces current consumption and increases battery life. Among the features of the PMT is the capability to monitor movement from locator to locator. A Guard Tour feature permits the system to monitor the time between arrivals at locations on a predetermined route, so that significant variations from the route and times of transit can create alarms. Actall offers two PMT versions: the PALS 9000 and the L2L.

Common Features of the PALS©® L2L and 9000:

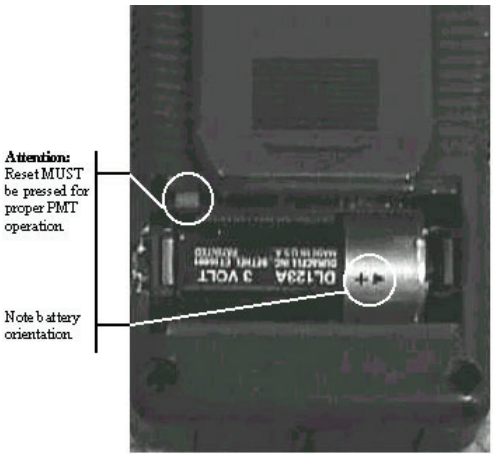
Push Button Alarm activation

Battery compartment/Reset switch: After a battery is installed in the PMT, the reset switch must be pressed. The switch is located inside the battery compartment, insid the cover above the battery holder.

Lapel Reader Accessory: The Lapel Reader is an infrared detector that may be plugged into the programming jack of the PMT and threaded through clothing that may inadvertently cover the PMT. The Lapel Reader has approximately the same IR sensitivity as the PMT and can be used to enhance IRT Locator reception. If the PMT must be worn under clothing, the Lapel Reader will function as a remote receiver for the PMT.

PMTs are powered by a disposable, 3V Lithium Ion battery. Typical battery life is 6 – 9 months for the PALS 9000 units and 4 – 6 months for the L2L, The L2L's battery life is less due to the additional IR Recevier circuitry in that model.

Lapel Reader



PMT Battery
Compartment and Reset

Additional Features of the PALS©® 9000:

- Pull Cord Alarm activation
- Man Down Alarm activation (internal tilt switch)
- 3-function slide switches on side:

  Position 1 (bottom) = Turns IR reader Off (supervision continues).
  Position 2 (middle) = Enables all features except Man Down.
  Position 3 (top) = Enables all features.

Operational procedures should be set in place to test the operation of PMTs and IRTs on a regular basis.

How IRT Locators Communicate with PMTs

Infrared transmitters (IRTs) send coded digital messages to an infrared receiver. Each message contains data identifying the IRT Locator ID. IRTs should be ceiling mounted on opposite sides of ingress/egress points between secure zones and/or in larger areas where location information is desired. Each IRT is powered by 12VDC and has a draw of 155ma. They are often set up in series from an aggregate DC power supply. Each PMT contains an Infrared receiver that reads valid IRT messages and decodes them. The location information is stored and rebroadcast via the radio frequency (RF) 900MHz transmitter.

Typical (Minimum) Computer System Requirements

Computer:	1.5 gHz Pentium 4 with 256MB RAM, 20GB hard drive, 48X CD ROM, 2 to 8 serial ports
Mouse:	PS2, or bus mouse
Monitor:	17" SVGA
Line Printer:	Optional (parallel port required)
Page Printer:	Optional (parallel port required)
Backup Power:	Optional
Network:	Optional (100Mb connections recommended)

How to Install the Software

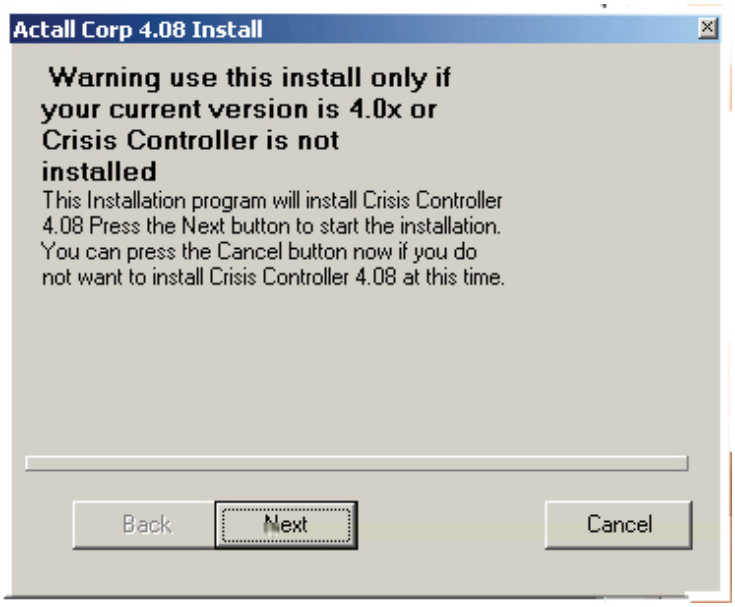
The Crisis Controller©™ software comes on a CD and can be used for either a new installation or upgrade of a previous version.

Prior to a new installation or upgrade of the Crisis Controller©™ software, verify that Crisis Controller©™ is not running, or in the process of upgrading either on the current machine or on a machine attached via the network. Irrevocable damage to your data may result.

To install the software on the hard drive:

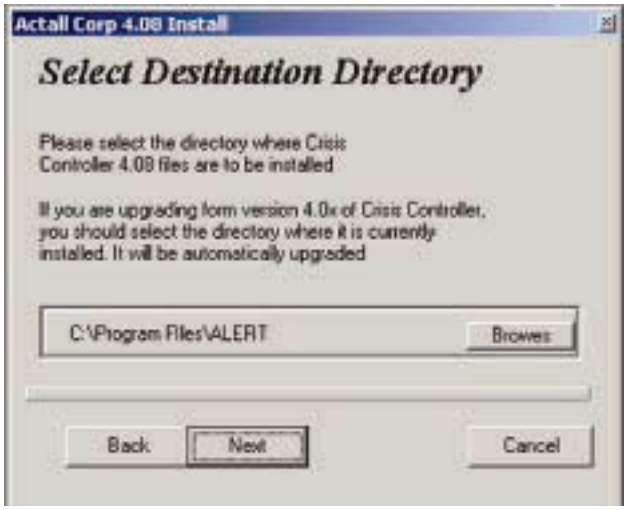
- Insert the CD into the drive.
- From the "Run" command, type "d:\setup" where "d" is the letter of the diskette drive.

The Setup program will assist you step-by-step in the installation or upgrade of the Crisis Controller©™ software. Please carefully read and follow the instructions during the installation. Once the questions are answered, the installation of the Crisis Controller©™ software will proceed automatically.



When upgrading from previous versions of Crisis Controller©™ software, some information cannot be converted due to limitations of current version. This information will have to be re-entered to maintain an identical system. You should consult an Actall Support Technician prior to upgrading any version of Crisis controller software.

The Setup program will prompt you for the directory where the Crisis Controller©™ files will be installed. If this is an upgrade, select the same directory as the previously installed Crisis Controller©™ software, this permits the appropriate files to be backed up as well as translated for utilization in the new software.



If this is a network installation, make sure the file server drive has been selected (i.e. F:\Program Files\Alert).

When you are ready to proceed, select Next. At any time you may select Cancel to abort the installation.

When the installation is complete, a file directory will have been created (the default directory is \Program Files\ Alert) as well as a Start Menu (the default start menu is Programs\Crisis Controller\Crisis Controller). You may place a Quick Start icon for Crisis Controller©™ on your Desktop. To do this, open the directory containing the program. Rightclick on the Alert icon. Select Create Shortcut, then drag the icon onto your desktop. See your Windows® instruction guide for further details.

The Crisis Controller©™ software can be networked either peer-to-peer or using a dedicated file server. In either case, each machine on the network running Crisis Controller©™ must have an Alert Monitoring Hardware Key installed at all times.

Warning:
All Hardware Keys must remain on the machines where they were initially installed and never relocated or removed for any reason. Doing so will cause undesired results and void all warranties implied or otherwise, unless specifically directed by Actall® Technical Support.

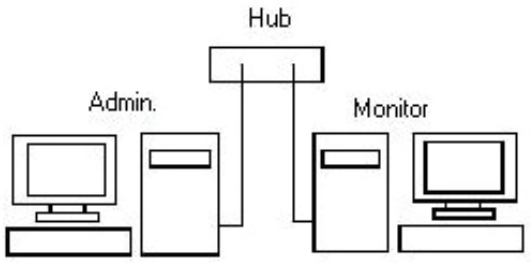
If you are unfamiliar with your operating system or you are unfamiliar with the intricacies of the network being used, please do not attempt to use the network function of the Crisis Controller©™. Doing so may cause permanent damage to your Crisis Controller©™ data files. Network installations should only be done by trained Network Technicians.

All connections in a Crisis Controller©™ networked system should be capable of no less than 100 Mb. In addition, all machines should be connected using a hub (or switch) rated at no less than 100 Mb.

The following is a guide for establishing the Crisis Controller Network only. All Network Hardware (Network cards and Hub/Switch) and appropriate drivers should be installed and their operation verified prior to proceeding to the Network setup for Crisis Controller. For instructions on establishing a peer-to-peer or client/server network, consult the required documentation on operating system being used for this configuration.

How to Install the Software

A peer-to-peer network is the most common method used for PALS installations. The network hardware should be connected and their operation verified prior to proceeding to the network installation of the Crisis Controller©™.



Peer-to-Peer Network

- Name each machine with a unique name (i.e. Monitor1, Admin 1, etc).
- Configure each machine to AUTOLOGIN to the Network. You should consult your operating system documentation for detailed instructions.
- The CPU named Monitor 1 will serve as the main server. Share the Crisis Controller directory, with full access, under drive properties [under NT, 2000, and XP you must also set access rights - See Operating System documentation for detailed instructions.] The Crisis Controller directory will consist of the installation path of the Crisis Controller©™ software (the default directory when the Crisis Controller©™ software is installed is: C:\Program Files\Alert).

- Verify that the Crisis Controller©™ software on each machine is installed into the exact same directory as the Monitoring Server (i.e. C:\\Program Files\Alert).
- Verify installation of Alert Monitoring Hardware Keys on each machine (the file server does require a hardware key). [See page 8 - Hardware Keys for detailed information.]
- On each computer, create a shortcut on the desktop that points to C:\ProgramFiles\Alert\alert.exe file. The best way to do this is by opening up the folder C:\ProgramFiles\Alert\, right clicking on the alert.exe file, select Send To, and then select Desktop (create shortcut)
- Close all windows that are currently open. Right click on the icon on the desktop labeled: “Shortcut to alert.exe”. Now left click on properties. A window will appear with a title of “Shortcut to alert.exe Properties”. Click on the Shortcut tab. Verify that the text box with the label of Start in: contains the path to the alert.exe program file (i.e. “C:\Program Files\ALERT”). Next, the text box with the label of Target: needs to be modified. The Target text box should already contain “C:\ProgramFiles\ALERT\alert.exe”. The following string needs to be appended to what is contained in the box: server=”\\servername\sharename” (quotations need to remain intact). An example of a valid Target command would be “C:\Program Files\ALERT\alert.exe” server=”\\servername\sharename”. Servername would be the name of your server, i.e. MONITOR 1, and sharename would be the name of the file share that is accessible from the network. Once all modifications have been done, click Apply, and then click Ok.
- Run Crisis Controller©™ from each machine by clicking on the shortcut that was created on the desktop.
- When prompted, enter a unique name for each machine (i.e. Monitor 2, Admin 1etc.). It is recommended that you use the same name chosen earlier.

The Monitoring Server and each machine should now be ready to run the Crisis Controller©™ software. You can verify the software has been installed and is operating correctly on the network by running the Crisis Controller©™ on each machine. Select Configuration > Utilities > Network Information from any active machine. The status of the network connections will be displayed by the name of each station. Verify that each machine is represented in the display.

When monitoring, the machine with the associated hardware (i.e. Serial Receiver) will display the alarm (if programmed to do so) immediately upon receipt of the alarm information. Other monitoring machines on the network will display the associated alarm (if programmed to do so) in approximately 7 to 14 seconds after the alarm was originally received.

Client/Server Network Configurations

Crisis Controller can also be configured to run in a Client/Server environment for large installations requiring this type of performance. An Actall Technician should be consulted prior to installing this type of network setup.

All Crisis Controller©™ systems will have at least one serial receiver and a number of transmitters. Every system must have an Alert Monitoring Hardware Key installed at all times. Other devices may or may not be used, depending on the application.

Hardware Key

The Alert Monitoring Hardware Key is a parallel connector with pre-set coded configuration that is also attached to the parallel port of the PC. It is a throughput connector so another parallel device, such as a printer, can be attached. The Hardware Key must be installed before attempting to install or activate the system. It cannot be removed after installation, as this will cause the monitoring system to terminate.

Installed Hardware Key

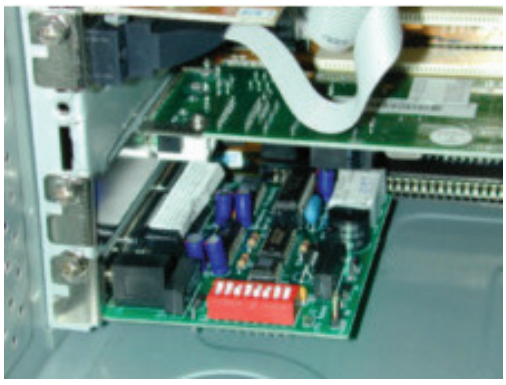
On network systems, Hardware Keys cannot be moved from machine to machine. Hardware Keys must remain on the machine on which they are originally installed. Make sure the side marked computer (the male connector) is inserted into the parallel port, NOT the serial port.

Serial Watchdog

The Serial Watchdog is a serial device that verifies the continued operation of a machine while monitoring. It is attached only by the card bracket; it is not in a card slot.

Installation:

The Serial Watchdog is installed into an open slot bracket on the monitoring system (not a slot in the motherboard). It is a throughput device, so the Serial Receiver attaches to the Serial Watchdog (if present) and the Serial Watchdog attaches to the serial port that is programmed for the Serial Receiver. [See page 10 for Serial Receiver installation information.] Connect the 2-pin reset header from the Serial Watchdog to the CPU RESET (pin 1 to pin 1 - watch orientation). If there is already a connector attached from the Reset button to the CPU RESET, you may attach it to the auxiliary connection on the Serial Watchdog controller. Connect the Serial Watchdog's supplied 4-pin Molex power connector to any available disk drive power receptacle.



Installed Serial Watchdog

Serial Watchdog DB9 Connectors

The Serial Watchdog includes an expansion unit that has a built in enunciator. It is set to 'ON' from the factory. To deactivate it, remove the shunt marked 'AUDIBLE'. If additional actions are required, should the watchdog activate, a Form 'C' reed relay is available. This relay is only rated for 100m VDC, so if a higher rating is required, an additional relay must be attached. Attach the expansion unit via the stereo jack to the Serial Watchdog. Attach the female DB9 connector to the computer serial port. Attach the male DB9 connector to the Serial Receiver, if present.

The DIP switches on the Serial Watchdog controller are factory set, they should not be changed for any reason. If they are inadvertently modified, contact Actall® Technical Support for assistance. There is no setup required for Serial Watchdog support in the Crisis Controller©™ software.

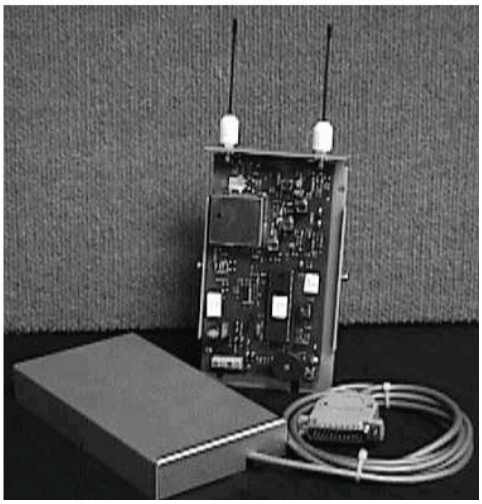
Once installed, the Serial Watchdog is activated by entering the Alarm Monitoring mode on that machine (only the machine with the watchdog is protected). It is sent commands using the same serial port as the Serial Receiver; therefore a Serial Receiver must be assigned in the Crisis Controller©™ software, regardless of it actually being attached. Should the Crisis Controller©™ fail to send the proper command every minute to the Serial Watchdog while in Monitoring mode; the Serial Watchdog will reset that machine.

On reset, the Serial Watchdog generates a momentary on-board tone and the expansion unit enunciator (if set to 'ON') will sound for approximately 30 seconds, during this period the reed relay will also activate.

After reset, the machine has approximately 3.5 minutes to reload Windows®, run the Crisis Controller©™ software, and return to Alarm Monitoring. If the system fails to re-establish monitoring, the Serial Watchdog will again reset the machine.

Once the Serial Watchdog has been activated, it will remain activated until Alarm Monitoring has been exited using the correct methodology.

Serial Receiver

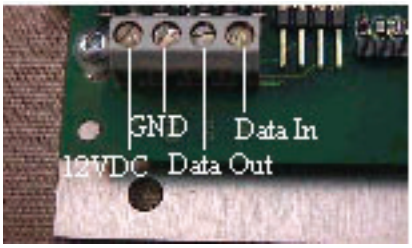


900MHz Serial Receiver

The Serial Receiver connects to a COM port (RS232 serial port) on the monitoring computer. The Serial Receiver translates digital signals from the system transmitters into a stream of serial data for the Crisis Controller©™ software to interpret.

Installation:

The Serial Receiver connects to the PC serial port using a 3-wire serial cable which has a DB25 or DB9 connector on one end (which is attached to the PC), and 3 loose connections on the other (which are attached to the Serial Receiver via its 4-position terminal block). The 3 loose connections attach as follows, pin 2 from the DB25 or DB9 to Data In, pin 3 to Data Out, and pin 7 to Ground.

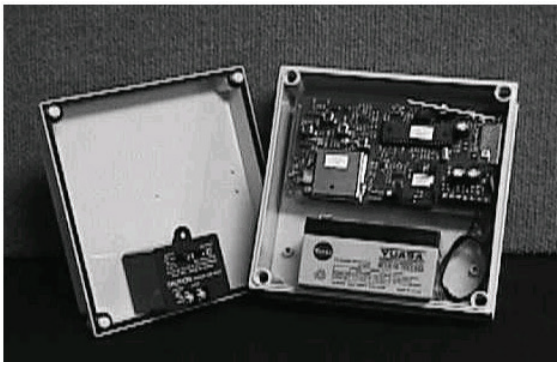


Serial Receiver Terminal Block

The serial protocols are not true RS232. However, the Serial Receiver will work with most standard PC serial ports which provide a +12VDC and -12VDC signal.

Once the serial cable has been attached, apply power via the included 12VDC power source. The Serial Receiver can be placed up to 150 feet from the PC. For greater distances, serial line drivers can be used. It should be mounted in a vertical position with antennas upright. It is recommended that the antennas should never come near metal objects.

Repeaters



Repeater

Repeaters need to be located for maximum contribution to the system. They should be located in areas where transmission strength is marginal. This can be determined by special signal strength measuring equipment (available through Actall® Corp.) or using Crisis Controller in “Test Mode”, which displays signal margin and signal level of each transmitter (see the Actall® User Manual). Repeater functions are not to be confused with IR or RF locating devices. Repeaters should be used when signal strength tests indicate marginal or weak signal conditions, or to provide redundant transmission pathways in critical sites. The RF transmission strength throughout any site should be determined by a site survey. The Repeater will re-transmit incoming weak signals at a higher strength. They can be used to extend the effective range of transmitters and to permit coverage of large sites. As many Repeaters as needed may be deployed, as special decoding features prevent “runaway” repetition of transmissions.

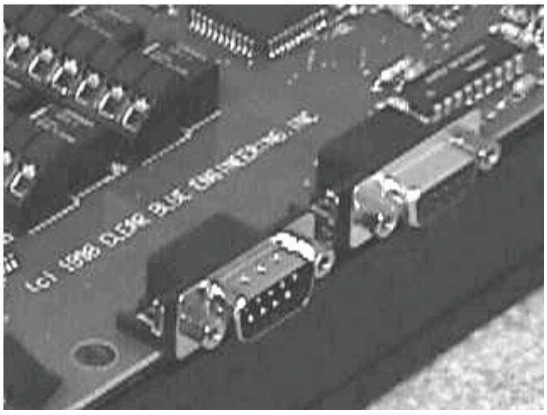
INSTALLATION:

Apply power via the supplied 14VAC transformer. Once power is applied, the Repeater can be programmed using the Crisis Controller©™ software and the Serial Receiver (see the Actall® User Manual). Once the Repeater is programmed it should be mounted on a wall or ceiling using a camera mount in a vertical position with the receive side of the Repeater facing the majority of the transmitters. The transmit side of the Repeater should be facing the Serial Receiver. The Repeater should never be mounted on or against a metal surface, as this will reduce its range.

Once installed, a 1.2AH backup battery can be added as a backup power supply. The Repeater will trickle charge the battery in approximately 48 hours. A 1.2AH battery should provide 4 to 8 hours of backup power.

INPUT /OUTPUT MODULE (SIO32)

The Input/Output Module (SIO32) is an external RS232 device that can be configured for both inputs and outputs. The SIO32 module connects to a serial port on the computer. Up to 8 SIO32s can be attached to each of 8 serial ports, giving users a potential of 2,048 input/output options.



SIO32 Serial Port

INSTALLATION:

Remove the housing cover of the SIO32 by removing the two screws from the top of the unit (screws are diagonal with respect to each other). Inserts in the cover can be removed from the Output and the Input end of the board to permit wiring to the terminals. Using the alternate diagonal holes, mount the SIO32 on a flat surface using the screws, washers, and anchors supplied with the unit. Be sure not to over tighten.

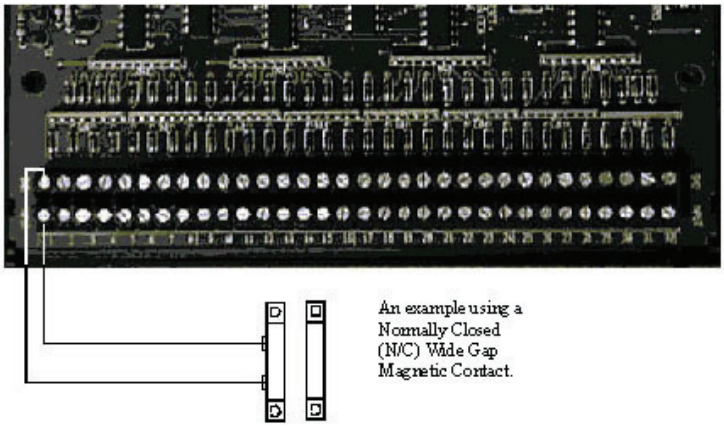
SIO32 Power Terminal Block

The SIO32 connects to the PC serial port using a standard serial cable that has a DB9 female connector on one end (which is attached to the SIO32 input marked “IN”), and a DB25 or DB9 male connector on the other (which is attached to the PC). If this unit is to be daisy chained (using the same serial port as a previous SIO32), a DB9 male to DB9 female will be required. Plug the DB9 female end into the previous units Output connector, and plug the DB9 male end into the new units Input connector.

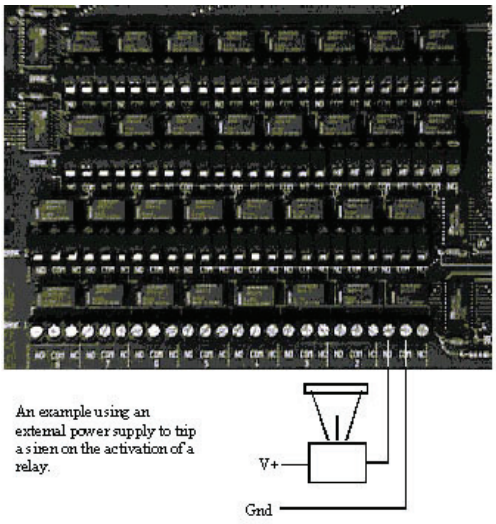
The SIO32 requires a 9 to 35VDC, 700mA power supply if any Outputs are to be used. If only Inputs are used, a power supply that supplies 300mA is acceptable. Connect power source Ground to the SIO32 terminal marked GND. Connect the Positive side of the power source to the terminal marked 9VDC. When power is applied, the PWR LED should light. If this does not occur, remove power and verify the connection. The receiver can be placed up to 25 feet from the PC. For greater distances, serial line drivers can be used.

The SIO32 Output section has 32 Form C relays, with connections arrayed in four rows of terminal blocks with N/O, N/C, and common terminals for each output.

The SIO32 Input section consists of two 32-position terminal strips with inputs on one side and ground terminals for each position on the other (ground terminals are on the inside)



SIO32 Inputs



SIO32 Outputs

CONFIGURATION: Configuration of the board is accomplished by setting the 8-position DIP switch.

Set Input or Output ("Off"=Output)				Set System ID + 1 ("Off"=0)			
Position 1	Position 2	Position 3	Position 4	Position 5	Position 6	Position 7	Position 8
Bank 1 Terminals 1-8	Bank 2 Terminals 9-16	Bank 3 Terminals 17-24	Bank 4 Terminals 25-32	MSB (Binary value = 4)	– (Binary value = 2)	LSB (Binary value = 1)	NOT USED

SIO32 DIP Switch Settings

Positions 1-4 set Input or Output options for the SIO32, in banks of 8. If switches are in the "Off" position, respective points are designated as Outputs. "On" sets them as Inputs.

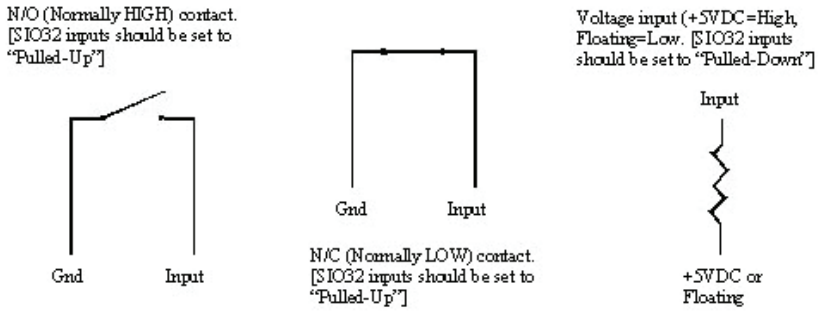
The same bank cannot be used for both Inputs and Outputs.

The next 3 positions (5 - 7) set the board ID, from 1 to 8. The associated ID is binary based plus 1 (000=1, 001=2, 010=3, 011=4, 100=5, 101=6, 110=7 and 111=8). Boards attached to the same serial port must have different IDs.

Any time DIP switches are changed, the Reset button must be pressed (located next to the DIP switches), or power to the SIO32 must be removed and reapplied.

ITo program the SIO32, see the Actall® User Manual. Programming identifies the module to the controller, and enables and integrates its function with the system. Outputs can be programmed to toggle states upon activation, or can be set to trip for defined momentary activation periods.

The Crisis Controller©™ software treats SIO32 Inputs like transmitters. They are defined as N/O or N/C (inputs controlled by switches are always pulled high). Switch transitions must be at least 25msec in duration. This permits "de-bouncing" of switches. Inputs can be tripped either by switch closure or by voltage changes. In addition, switches can be programmed to directly trip outputs.



N/O and N/C Circuit

Paging

The Crisis Controller©™ can automatically respond to alarm or trouble events by automatically communicating with on-site or off-site pagers. Users can also manually activate specific pagers as needed (see Actall® User Manual for additional details).

The system accommodates multiple pager services, with service to all types of pagers. When programmed or manually instructed to send a page, the system calls the pager service assigned to the pager and relays numeric or alphanumeric information. This paging interface requires a connection via a COM port.

Installation: Due to the versatility of the many paging systems available, please see the manufacturer's documentation for hardware installation and programming.

Printer

The Crisis Controller©™ will support a dedicated line printer that will produce real time printouts of system activity, or can be used with a standard printer with reports being requested by Operators or Supervisors.

Installation: Attach the printer to the parallel port of the PC using a standard parallel printer cable. With one end attached to the printer, attach the other end to the Alert Monitoring Hardware Key.

Wireless Transmitters

Transmitters should not be mounted on-site until they have been programmed and labeled for easy identification in the field. Transmitters are programmed from the Alert Monitoring Center using a programming cable connected to the Serial Receiver

INSTALLATION: Batteries must be installed in transmitters before programming. Specifications and related programming instructions for each type of transmitter are included in the literature packed with the unit.

The Crisis Controller©™ permits users to test signal strength of individual transmitters that can send signals directly to the Serial Receiver without the use of a Repeater. If Repeaters are used, either a Survey Kit is required (available through Actall® Corp.) or the Crisis Controller©™ software must be installed on a portable machine allowing for mobility. Please contact Actall® Technical Support for more information.

RF signals change with the environment, so signal strength measurements cannot be relied on solely. Complete supervision of the transmitters and frequent testing should be the main course of action to ensure a working system.

IRTs, PMTs, and Wireless RF Locators

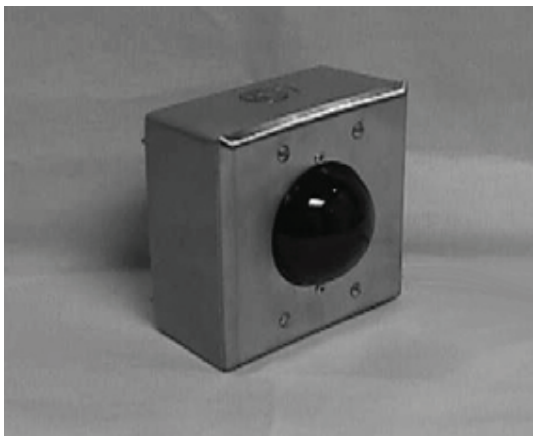
The Crisis Controller©™ software is often used in applications involving mobile transmitters carried for personal protection, by guards or watchmen. In these applications, it is extremely valuable to have a system that not only responds to alarms, but can also provide information on the location of the personnel carrying the transmitters. The Crisis Controller©™ has several answers to this challenge.

IRT Locators

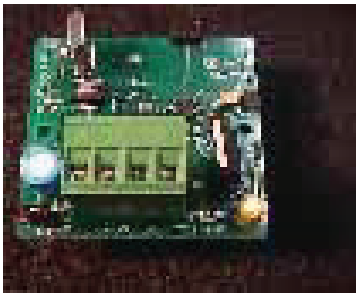
IRT Locators are special infrared transmitting devices that generate an ID code and are received by the PALS©® 9000 Personal Mobile Transmitters (PMTs). IRT Locators transmit identification codes to PMTs carried by authorized personnel.

The ID code is used to identify the alarm location or zone from which the alarm originated. Location information is subsequently encoded into the transmissions from the PMT to the PALS©® Alert Monitoring Center. It is then possible to monitor position and movement of the individuals on-site.

IRT Locators continuously transmit locator data code via infrared light. The PMT includes an infrared receiver that is activated at regular intervals. If the PMT is within the coverage area of a Locator, infrared data is read and stored in the PMT, then included in status transmissions to the PALS©® Alert Monitoring Center.



IRT Transmitter Enclosure



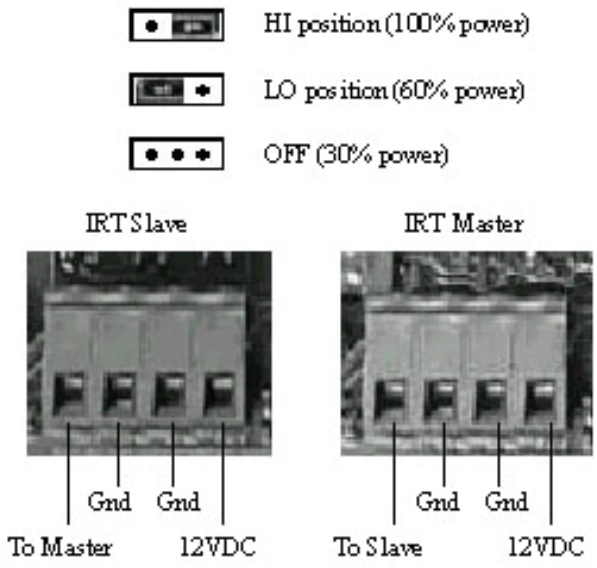
IRT devices may be single units, or can consist of combinations of Master Locators (IRT-M) tied to a number of Slave Locators (IRT-S), all of which transmit the same data and create a single zone to provide saturation coverage of an area.
The reliability of a Locator depends upon the capacity of the alarm transmitter receiving data in a given area. Infrared signals have some transmission limitations that can be overcome by careful placement and use of Master-Slave combinations.

IRT Locators (Master and Slave) require 12VDC (300mA) power supplies and can be interconnected with 24-gauge wire in 4-conductor cable.

PROGRAMMING OF IRTS: Use the PALS©® IRT 60703 Tester to program. Detailed instructions on the use of the 60703 are included with that device.

4-POSITION TERMINAL BLOCK: Positions are 12VDC, Ground (IRT Master power), and Ground and Slave power (for powering Slave units.) Master IRTs have a red power-on LED indicator. Slave IRTs have a power-on LED as well as an LED to indicate proper connection with a Master IRT. Slave IRTs require individual power sources. A single power source can operate a Master and up to 5 Slaves, if power supply is adequate. Master and Slave Locators should be connected with 3-conductor 24 to 22-gauge wire. Total combined wire run between Master and Slaves should not exceed 400 feet.

3-POSITION HEADER: Determines a "high", "lower," and "lowest" power setting for IRT range. With the jumper in the "HI" position, the unit operates at 100% power. With the jumper in the "LO" position, the unit operates at approximately 60% power. With the jumper "Off," the unit operates at approximately 30% power. Power selection is used to reduce range to prevent adjacent IRT zones from overlapping, creating null transmission areas.



IRT 4-Position Terminal Block and 3-Position Header

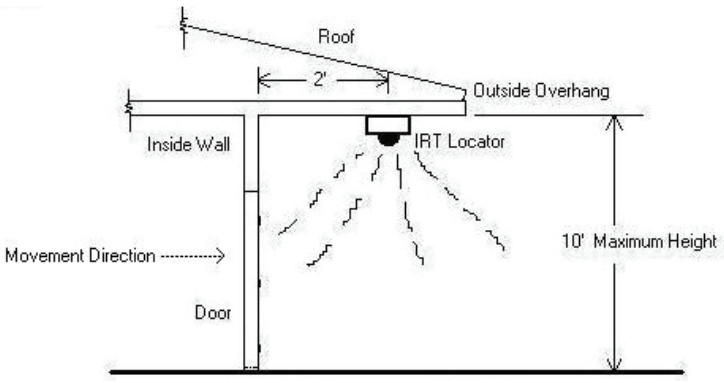
INFRARED LENSES: Most infrared lenses will reduce the signal by 3 to 7%. The optimum lens for the IRT-M and the IRT-S is no lens at all. However, as this is not practical, it is very important to use only lenses specified (and included) by Actall® Corp.

Programming IRTs into Crisis Controller: After configuring and wiring the IRT Master units, IRTs must be programmed into the Crisis Controller©™ software. Programming identifies the IRT to the controller, and enables and integrates its function with the system.

Once IRTs have been programmed in the Crisis Controller©™, they are accessible to the Guard Route feature, and can be included in a timed and sequenced patrol path.

Coverage and placement of IRT Locators:

The guiding principle of installing IRT Locators is that signals to PMTs will be unobstructed and unambiguous. Wherever IRTs are used, the PMT must be able to get ONE clear signal at a time. This means that IRTs must be located in such a way that users will always be in range of a PMT and that signals from one IRT can always reach the PMT.



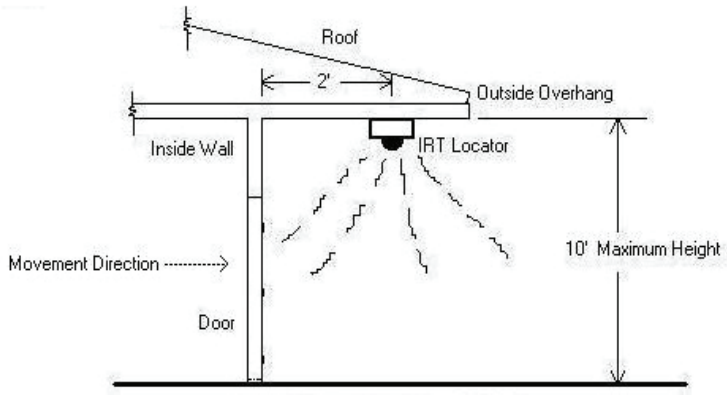
Ceiling Mounted IRT (Side View)

Several factors must be considered. First is range; the effective transmission range of an IRT is a function of its total peak output power. IRTs have jumpers that permit users to use a low power output, which reduces range. This is sometimes desirable as a means of limiting overlapping fields of coverage between adjacent receivers.

The next factor is location of the IRT device. Users typically carry PMTs on belts or service holsters. Signals to the PMT can be shielded, or "shaded," by the user's body if the PMT is worn on the side of the user opposite the location of the IRT. This situation is addressed by using sets of IRTs. IRT Slaves may be operated in conjunction with IRT Masters. They transmit the same location data as the Master, at 5%-10% lower power. Strategically placing these devices in an area guarantees that Locator signals can reach a PMT regardless of where the wearer is carrying the PMT, or which direction the user is traveling. (If users must wear heavy protective gear, use of a Lapel Reader with the PMT is recommended.)

IRTs transmit data in 3-dimensions. Coverage may be envisioned as a "cloud" of signals through which the PMT must pass. IRT signals disperse from their source, and are often augmented by signal reflection from most materials. (Carpets and black surfaces are poor reflectors).

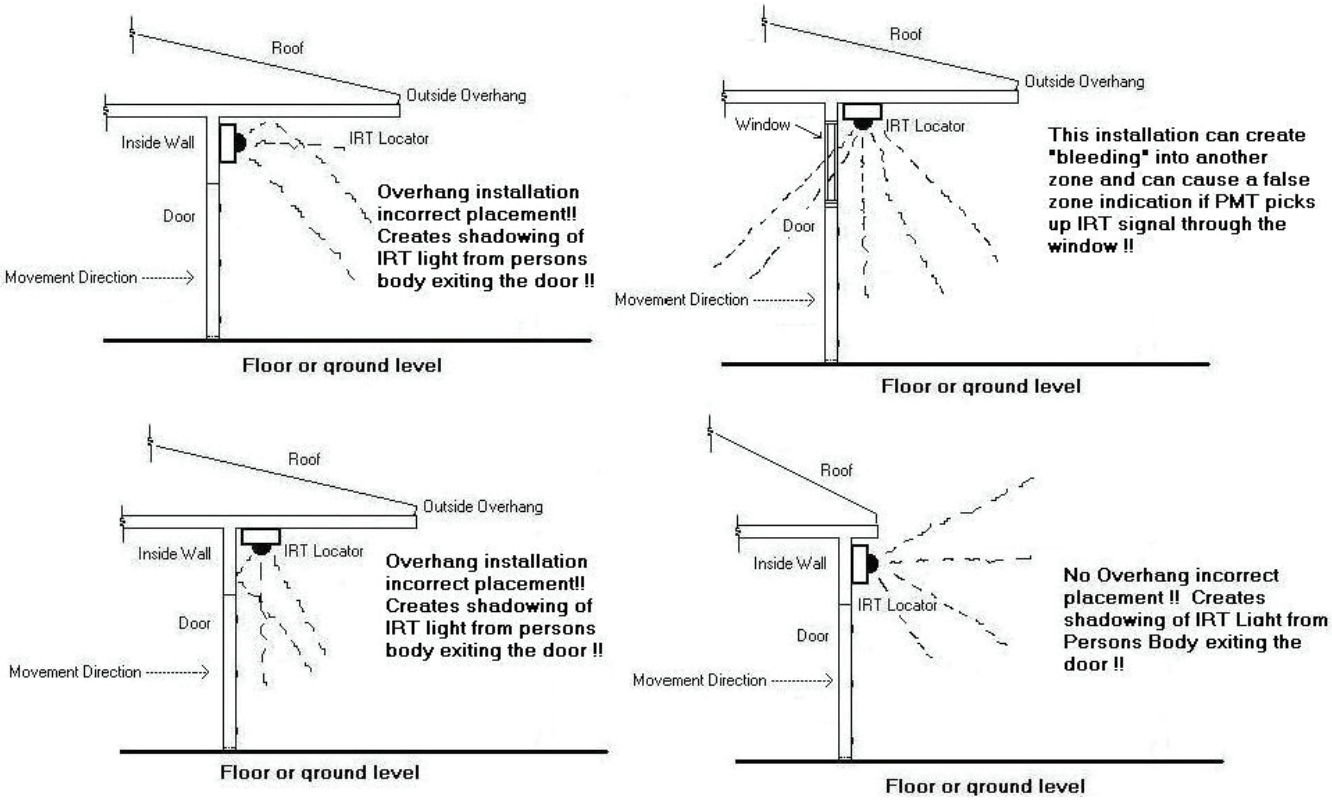
Installers should place IRTs to eliminate overlapping zones of dual coverage. When signals from adjacent IRTs collide, "dead zones" are created, from which no viable information is accessible to the PMT.



Door Mounted IRT (Side View)

IRTs are not affected by exposure to sunlight, but PMT receivers can be saturated with environmental IR and cannot read the Locators. In these cases, installers should locate the IRTs in areas that the PMT will not be in direct sunlight when the Locator data needs to be received.

IRT range can be reduced by proximity to fluorescent lighting. Generally speaking, loss is minimal if the IRTs are farther than 2 meters from the light source and the light source is not generating in-band noise. In-band noise is typically generated by an electronic ballast. IRTs must be mounted per the diagrams shown. Incorrectly mounting the IRTs may significantly reduce the range or inhibit the operation of the unit. The following are four examples of incorrectly mounted IRTs.



Incorrectly Mounted IRTs (Side View)

Wireless RF Locators (RFL)

Another method of determining location of PMTs is through Wireless RF Locators. These devices are 900MHz transceivers that attach data to transmitter messages indicating which Locator device was the first to pick up a signal directly from the transmitter. Wireless RF Locators are typically used to provide approximate origination signals from PMTs. Wireless RF Locators provide relatively coarse indications of location, partly due to their extensive range. They are particularly well suited for outdoor zoning with the PALS©® transmitters.

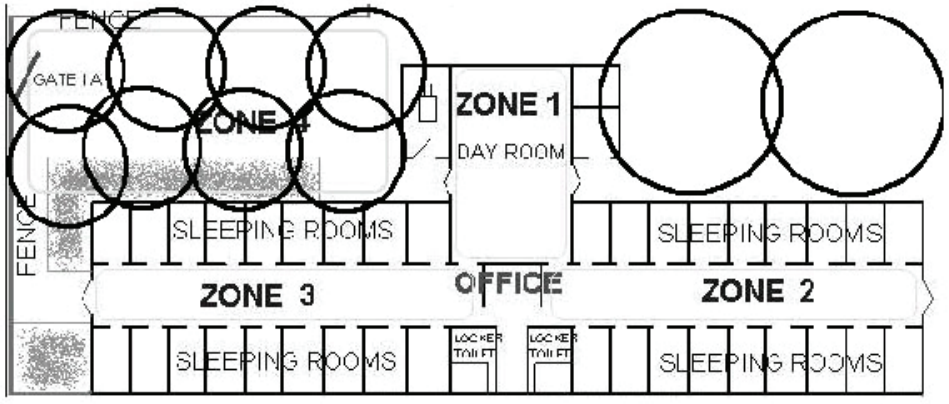
Wireless RF Locators can be used very effectively in conjunction with IRT Locators. For example, IRT Locators can be used to closely monitor movement inside a building. They can be programmed to indicate when personnel enter or leave an IRT-supervised area. If personnel need to move between buildings, for example, RF Locators can provide larger area coverage while they are in transit. When they enter another building, IRT sensors will note their arrival.

Unless the system is advised that a user has exited an IRT Locator zone, it will not look for RF Locator transmissions. Once the user passes the exit IRT, the system will begin to look for incoming data from RF Locators. Exit units should be placed at doorways or passageways leading into areas covered by RF Locators. In the figure below, for example, exit units should be installed at the doors out of the Day Room, and at the doors at the end of the long hallway, if they are used for egress to the areas outside the building.

Wireless RF Locators must be used in conjunction with IRT exit points on the PALS©® 9000. Due to the characteristics of RF and the tolerances of the Wireless RF Locator, it is very likely that RF Locators will need to have overlapping coverage. This means that it is also very likely that more than one RF Locator will receive a given message. Because of this, there is a brief delay in the Crisis Controller©™ software when reporting any potential RF Locator messages. In addition, because the RF Locator is based on its RF sensitivity, if not properly adjusted, a missed signal is possible.

For "FINE" coverage, the RF locator sensitivity pot should be set to 60.

Note: Overlapping coverage should always be provided, as RF signal paths will continually change.



For "COARSE" coverage, the RF locator sensitivity pot should be set to 100.

RF Locator Coverage

After the Crisis Controller©™ software has been successfully installed and tested, routine maintenance tasks can be performed by trained supervisors.

Troubleshooting

Problems that appear related to hardware or programming should be referred to the installer. Below are typical maintenance issues that can arise during operation of the Crisis Controller©™ software. For additional support, operation, or installation difficulties contact Actall® Technical Support at 303-487-4222 Monday through Friday, 8:00 a.m. to 5:00 p.m. Mountain time or Email technicalsupport@actall.com.

Transmitter Problems

Wireless transmitters are battery powered. Battery life on most products is estimated in years and should not pose a problem. When batteries do begin to fail, however, transmitters will report this to the software and a trouble warning will be generated in time to replace the battery. Some transmitters can be protected against tampering. Tamper switches or end of line resistors can cause a trouble warning to be generated, indicating that the transmitter has been damaged or disturbed. Make sure when programming transmitters, after attaching the programming cable to the 3-pin header, the reset button is pressed.

PMTs

PMT battery life can be extended by turning the PMT off when not in use (move the slide switch to position 1). When the PMT is off, it continues to report supervision information to the Serial Receiver.

Receiver/Repeater Problems

Receivers and repeaters are highly reliable. Typically, if there is a problem it appears as a receiver or repeater failure, and is noted in the monitoring log. Failure of power sources and backups, wiring disconnection or inadvertent reassignment of COM ports can all cause a trouble warning to be generated. For improved RF range, make sure to mount the receiver in a location that is RF friendly (no metal back plates or back boxes).

IRTs

Communication between IRTs and PMTs is very reliable. If an IRT is not providing the correct address, make sure the DIP switch is set correctly and the power supply is providing the proper amount of current.

After the Crisis Controller©™ software has been successfully installed and tested, routine maintenance tasks can be performed by trained supervisors.

PMT Specifications

Peak Current:	30mA
Frequency:	900MHz
Maximum power output:	10mW
RF Open field range:	2500 feet

Lapel Specifications

Peak Current:	3mA
Connection:	Shielded stereo cable
Conductors:	2 plus shield

IRT-M Specifications

Supply, Master IRT Locator:	10-15 VDC @ 300mA
Current with jumper in HI:	155mA
Current with jumper in LO:	75mA
Current without jumper:	25mA
Maximum power dissipation:	2 watts
Open field range with jumper in HI:	125 feet
Open field range with jumper in LO:	80 feet
Open field range without jumper:	40 feet

IRT-S Specifications

Supply, Slave IRT Locator:	10-15 VDC @ 300mA
Current with jumper:	130mA
Current without jumper:	65mA
Maximum power dissipation:	2 watts
Open field range:	5-10% less than Master IRT

SIO32 Specifications

Supply:	9 VDC to 35 VDC @ 700mA
Form C Relays:	35 VDC @ 1A
	120 VAC @ .5A
	60 VDC @ .3A
Input sync current:	80mA
Maximum power dissipation:	3 watts
Input Connection:	DB9 Male
Output Connection:	DB9 Female
Maximum # per Serial Port:	8

Actall Corporation
ISO 9001:2015 Certified

Actall Corporation
2017 Curtis Street | Denver, CO 80205
www.actall.com 303-226-4799