



Excellence in Compliance Testing

Certification Exhibit

**FCC ID: Q6K-MCU102A
IC: 5043A-MCU102A**

**FCC Rule Part: 15.231
IC Radio Standards Specification: RSS-210**

ACS Report Number: 10-0184.W06.11.A

**Manufacturer: 3Si Security Systems
Model: MCU-102A**

Manual



Octopus[®] Installation & User Manual

Last Updated: 06/07/2010



Table of Contents

How To Use This Guide	3
FCC Statement	3
Octopus® System Description.....	4
System Overview	4
Operational States	4
Disabled State	4
Enabled State	5
Arming Delay State.....	5
Armed State	5
Activation State.....	5
Daily Operating Procedure.....	5
System Maintenance	5
Octopus® Components	6
Monitor and Control Unit (MCU).....	6
Cassette Staining Unit (CSU).....	8
iButton Reader	10
Appendix A – Preparing for Installation.....	A1
Appendix B – Installation Report	B1
Appendix C – Installation Procedures	C1
Appendix D – Managing iButton Keys	D1
Appendix E – Serial Communications Access	E1
Appendix F – Optional Features	F1
Bank Alarm Interface.....	F1
Internal Siren.....	F1
Breach Sensor.....	F1
Note-Stop	F3



How To Use This Guide

This guide is designed to introduce you to the features of the 3SI Octopus[®] ATM Defense System and to assist in installation and operation. Due to the numerous variations in currency cassettes, procedures for the cassette installation are provided in separate documentation.

The section on system description includes a brief background of the Octopus[®] system, definition of the various operational states, daily operating procedures and system maintenance. The appendices give further technical details for installation, and other specific procedures for operation and management of the Octopus[®] system.

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this equipment may not cause harmful interference; and (2) this equipment must accept any interference received, including interference that may cause undesired operation. This equipment generates, uses, and can radiate radio frequency energy, and if not properly installed and used in accordance with the manufacturer's instructions, may cause harmful interference to radio communications. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Warning: Any changes or modifications to this device not expressly approved by 3SI Security Systems could void the user's authority to operate the equipment.



Octopus[®] System Description

System Overview

The 3SI Octopus[®] ATM Defense System is a patented wireless system designed to protect automatic teller machines (ATMs) from theft (pull-out) and break-in attacks. The system is comprised of three main components: a Monitor and Control Unit (MCU), up to 6 Cassette Staining Units (CSU), and an iButton Key Reader. The MCU is located in the main ATM safe area, and monitors the ATM for theft or break-in. The CSU is located within the currency cassette, and provides the ability to stain the currency in the event of attack - thus rendering the money useless to the attackers. The iButton Key Reader provides a secure method of accessing and controlling the MCU state (as defined below), and contains an LED to provide status of the present operational state (see below). The system is designed for continuous monitoring and protection of cassette-based ATM currency for a period of two years without system maintenance or service interruption.

The MCU is powered by a plug-in Power Adapter, but also has an internal rechargeable battery which will provide backup in case of power loss. The CSUs are powered by an internal battery pack which provides maintenance free operation for a full two years. The small dimensions of the MCU allow it to be placed almost anywhere within the ATM safe, while the small bracket design of the CSU allows for fast field installation with minimal cassette modification.

The Octopus[®] system offers two modes of protection:

- **Auto-Arm mode** - Auto-Arm mode is the default mode, and provides for theft (pull-out) protection only.
- **Door-Bolt mode** - Door-Bolt mode is optional, and provides additional protection against break-in by monitoring the proper opening/closing of the door dead-bolt. The door-bolt option must be specified at the time of ordering since additional installation components are required.

The Octopus[®] system offers several optional features to enhance the detection and alarm capabilities of the system. (Refer to Appendix F for details.)

Operational States

The Octopus[®] system has 5 operational states: Disabled, Enabled, Arming Delay, Armed, and Activation. Each of these states is indicated by a specific iButton LED color:

Disabled State – LED Off

When in the Disabled state, the system is essentially OFF and will not monitor for an ATM attack. The Disabled state is the only state in which serial communications can be established with the MCU via the computer serial port.



Enabled State – LED Green

The Enabled state is applicable only to an Octopus[®] system operating in the Door-Bolt mode. When both the door and door dead-bolt have been properly opened, the iButton LED will turn green indicating that the system is enabled but not armed. The system proceeds to the armed state (see below) when both the door and door dead-bolt are properly closed.

Arming Delay (or “Pre-Armed”) State – LED Flash Red / Green

Prior to arming there is a delay called the “Arming Delay”. The delay is 5 seconds for Auto-Arm mode, and 5 minutes if the optional Door-Bolt mode. During the arming delay the system is not monitoring for an attack, and the iButton LED will flash red then green.

Armed State – LED Red

When in the Armed state, the system is monitoring for attack. The iButton LED will be red. If the ATM is attacked, the system will activate (see below) and stain the ATM currency.

Activation State – LED Rapid Flash Red

When the system has detected an attack on the ATM, the MCU commands the CSU to activate and stain the currency. The iButton LED will rapidly flash red. The activation state can be reset by using an iButton Key (see iButton description below). In addition, the following optional features will activate (refer to Optional Features, Appendix F):

- **Optional Bank Alarm Interface:** If configured for external bank alarm interface, the MCU’s normally closed contacts will open, thereby activating the external bank alarm.
- **Optional Internal Siren:** If the Internal Siren is installed, the siren will sound on activation. After 15 minutes, the siren will cease.
- **Optional Note-Stop:** If the Note-Stop module is installed, the ATM will be disabled and will not dispense bills.

Daily Operating Procedures

Regardless of the protection mode being used (Auto-Arm or Door-Bolt), normal daily operating procedures for the ATM itself are not affected. The Octopus[®] system will automatically arm and disarm as the machine is serviced and money cassettes are replenished.

If physical repair of the ATM is required, maintenance personnel should be made aware that an anti-theft protection system is installed. Prior to beginning the ATM repair, the Octopus[®] system should be disabled via the iButton Key (see procedures below).

System Maintenance

No special maintenance is required for the Octopus[®] system for a period of two years.

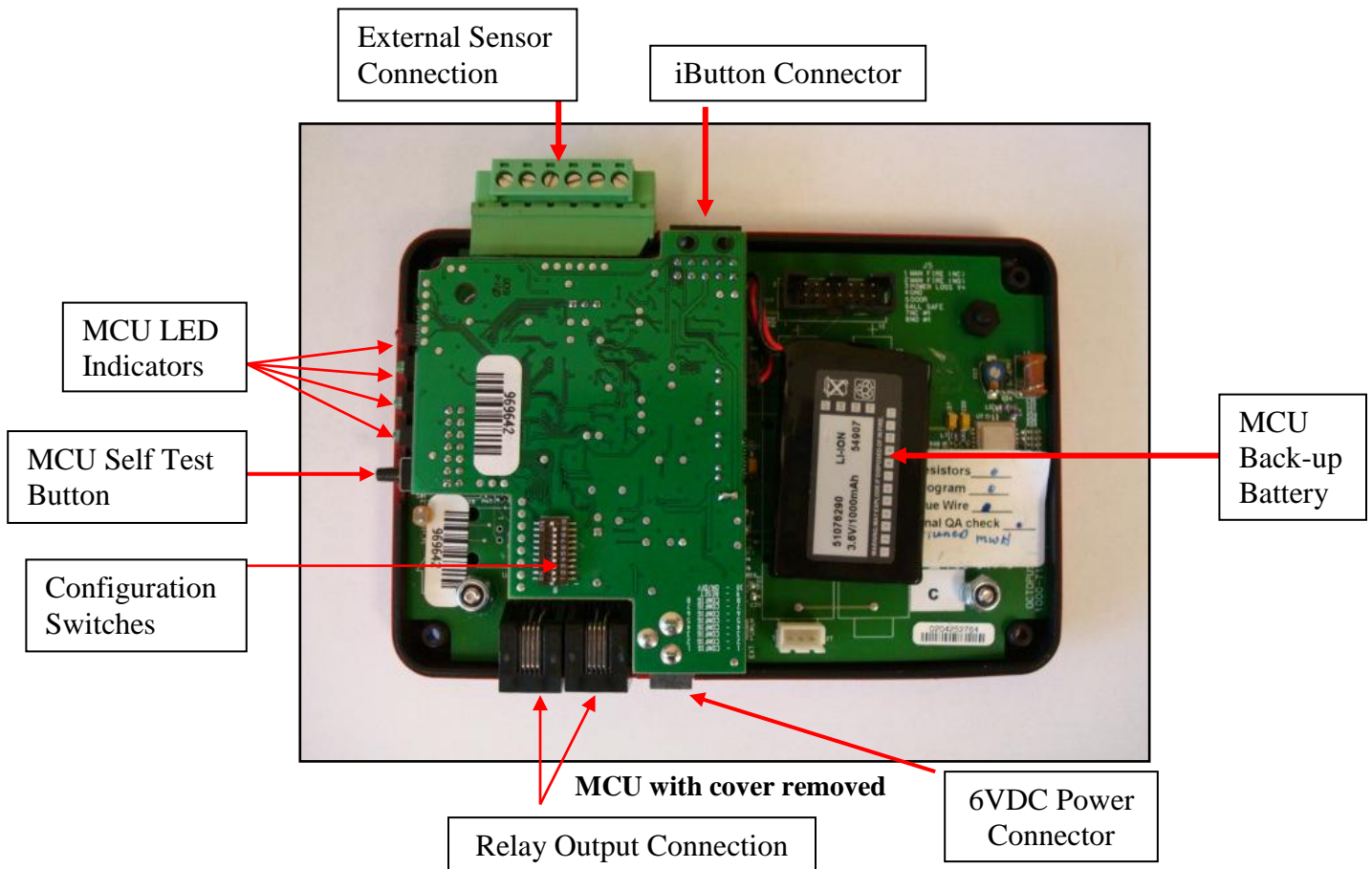


Octopus[®] Components

The Octopus[®] system has 3 major components: the Monitor and Control Unit (MCU), the Cassette Staining Units (CSU), and the iButton reader.

Monitor and Control Unit (MCU)

The Monitor and Control Unit (MCU) is mounted inside the ATM safe. The purpose of the MCU is to monitor the status of the system and to control the activation of the Cassette Staining Units (CSU) and other optional features. The MCU is enabled or disabled using an I-Button Key (see iButton description below). The MCU monitors tilt violation, proper door and door-bolt opening (if configured for the Door-Bolt mode), and integrity of the optional breach panel. When the system detects an attack, it directs the CSUs to activate and stain the currency, and also activates any optional alarm features.



Power Supply & Backup Battery

The MCU is powered by a UL approved plug-in 6 VDC power supply (1Amp minimum rating). It also has a back-up battery to maintain power in the event of an ATM power loss. The battery will provide backup power for approximately 3 weeks.

Self Test Button

On initial power up the MCU performs a self test routine. The MCU is also provided with a Push-To-Test (PTT) button which causes the unit to perform a self diagnostic test. If the test returns no errors, the MCU will beep 1 time. (See Installation Procedures for diagnostics information.)

The MCU self test also sends a test message to the CSUs. The CSU will perform its own self diagnostic, and return 1 beep for no error and 2 beeps to indicate an error.

LED Indicators

The MCU has 4 LEDs that indicate the status of the various inputs. (See Installation Procedures for details.)

NOTE: The LEDs are only active when the MCU is in the Disabled state and operating on external power.



MCU front panel

External Sensor Connection

The MCU may be connected to optional Door/Door-Bolt switches and Breach Panel sensor. Connection is made via a terminal block on the side of the MCU. The terminal block may be removed for easy wire connection. (See Installation Procedures for wiring details.)



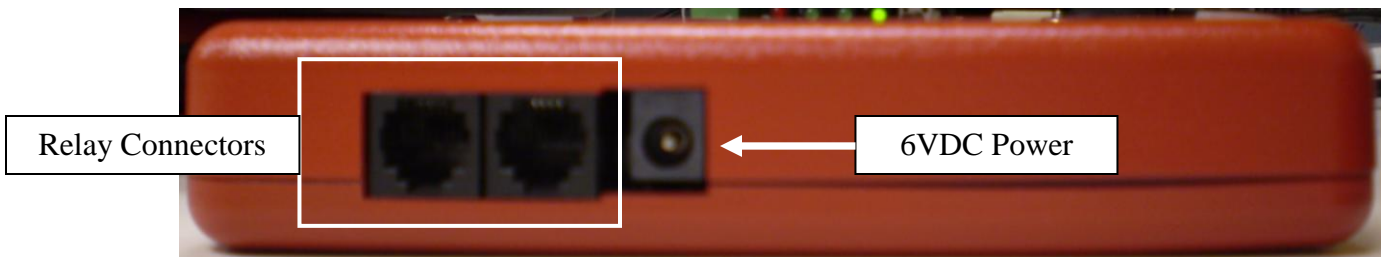
MCU side view with iButton/serial interface connector and ext sensor terminal block

Connector (iButton)

The iButton Connector is a locking, polarized 10-pin connector. This connector is used to attach the cable from the iButton reader to the MCU. (Refer to the iButton reader description below)

Relay Output Connection

The MCU has two RJ11 output jacks which provide relay interface to the optional accessories such as: Internal Siren; Bank Alarm Interface; ATM Note-Stop. Both jacks are identical in function and pin-out. (Refer to Installation Procedures for wiring details.)



MCU side view with RJ11 connectors and 6VDC Power Connector

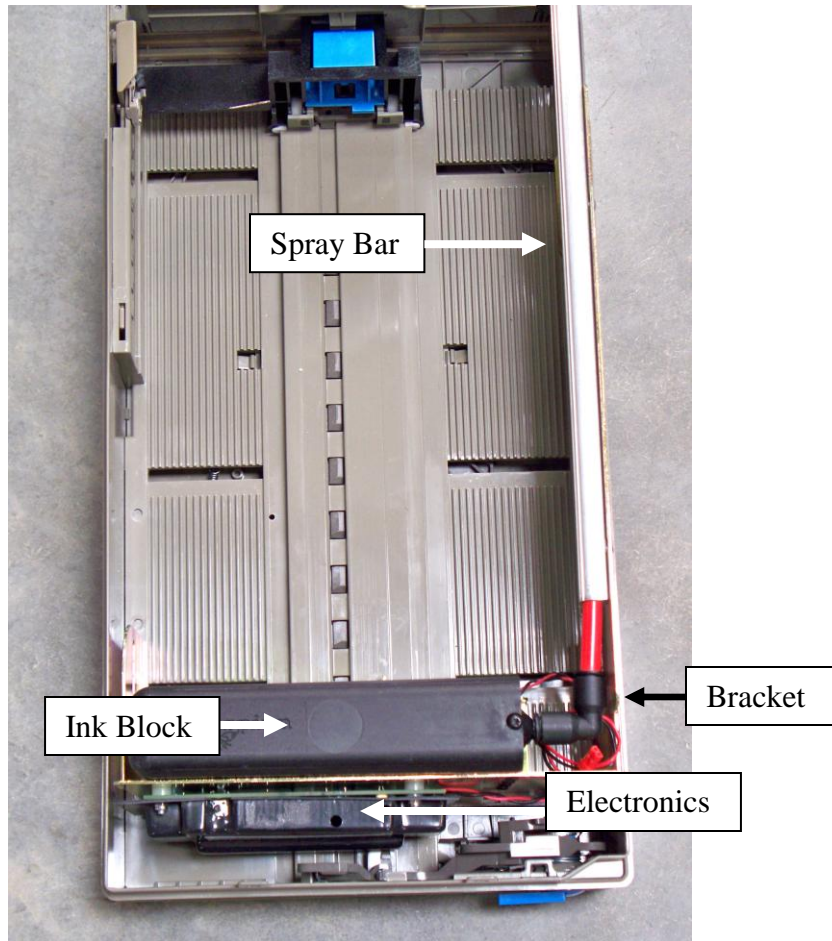
Configuration Switches

The 10 MCU Configuration Switches are used to configure the operating mode and options for the system. (Refer to the Installation Procedures for details.)

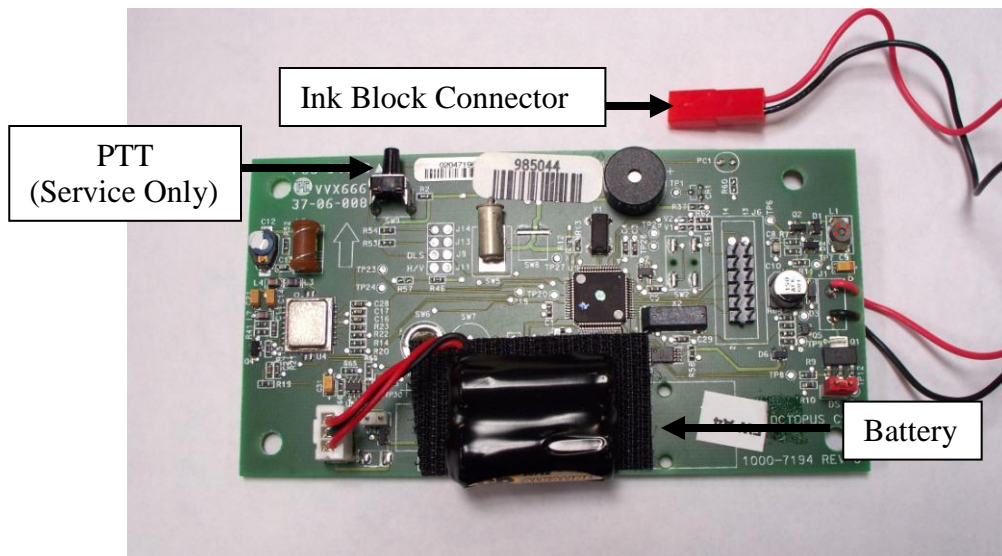
Cassette Staining Unit (CSU)

The Cassette Staining Unit (CSU) is mounted in each of the ATM currency cassettes. The CSU utilizes a small profile mounting bracket unique to each make/model cassette. The CSU is comprised of 4 components: Electronics, Ink Block, Spray Bar, and Mounting Bracket. The link between the MCU and CSU is via a proprietary patented radio frequency (RF) communications link.

The CSU contains an internal battery pack which will provide power to the CSU for two years. The CSU Push-To-Test (PTT) button is for use by service personnel only. Once installed in the currency cassettes, no action is required by the user.



CSU Installed in Cassette



CSU Electronics

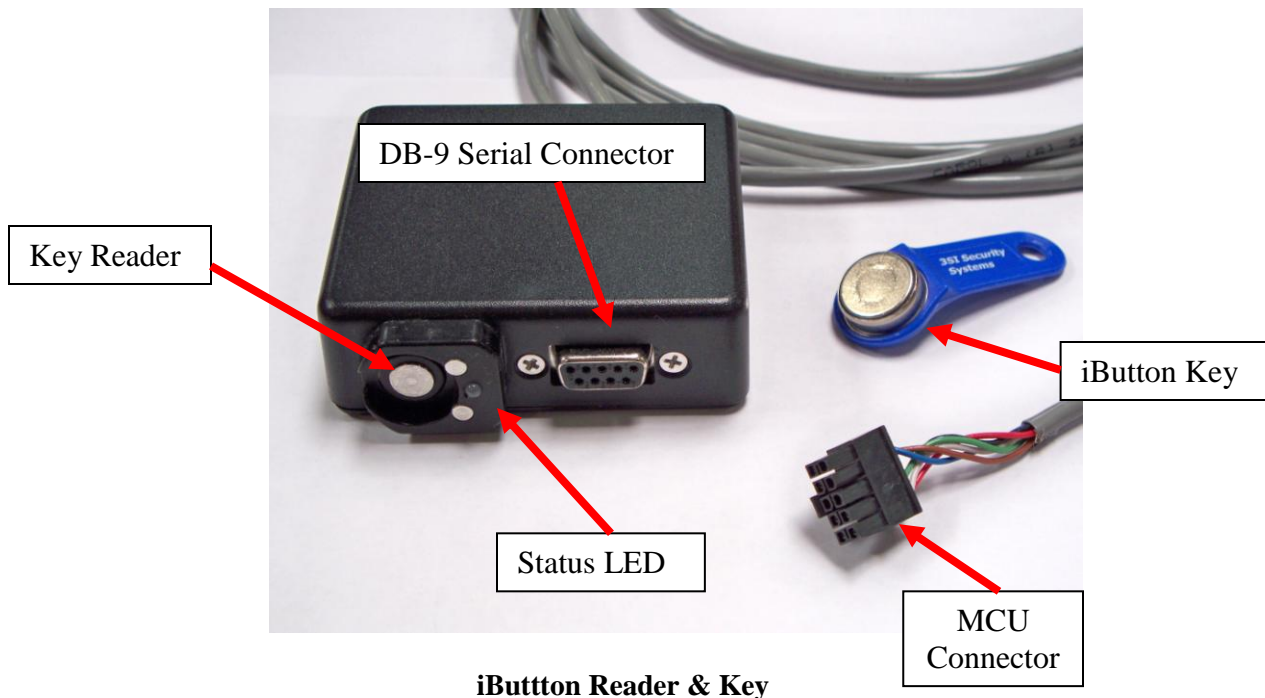
iButton Reader

The iButton reader is used to enable and disable the Octopus® system via the iButton Key. The iButton DB-9 serial interface connector provides a computer interface for initial system setup, and for retrieval of the system event log. The iButton Reader is mounted outside of the actual ATM safe, but inside the ATM enclosure in an area that is readily accessible during service. The iButton Reader is wired to the MCU via a multi-conductor cable.

The bicolor LED on the face of the iButton reader indicates the status of the system. When using normal external AC power the LED color is solid. When operating on backup power the LED color flashes. Table 1 below shows the iButton LED indications for the various system states.

Table 1. Octopus® States and Corresponding iButton LED Color

Octopus® State	LED Color
Disabled	LED is not lit
Enabled but not Armed (Door-Bolt Mode only)	Green
Arming Delay	Alternating red/green prior to arming
Armed	Red
Activation	Rapidly blinking red



Appendix A – Preparing for Installation

Each installation has its own special requirements depending on the system configuration and options selected.

The following configuration options and requirements must be determined prior to installation:

- Mode of protection required (Auto-Arm or Door-Bolt)
- Make and model of ATM
- Type and number of Cassettes to be protected
- Requirement for Breach Sensor Option
- Requirement for Note-Stop Option
- Requirement for other alarm options: Internal Siren, Bank Alarm Interface

Cassette Assembly

The installation of all CSUs and ink blocks in cassettes must be completed before installing the Octopus[®] System in the ATM. Installing the CSUs in cassettes beforehand minimizes down-time during the Octopus[®] System installation.

NOTE - Important: The CSU Ink Block connector must not be connected until the Octopus[®] System installation is complete, and all tests have been run.

Field Logistics

It is important to define all personnel involved and their respective responsibilities prior to beginning the Octopus[®] installation. (Refer to table below)

Field Logistics / Responsibilities:

Personnel Involved	Responsibility
Supplier Project Manager	<ul style="list-style-type: none"> ▪ Develop the installation schedule with the Customer Project Manager ▪ Provide installation reports upon request ▪ Coordinate policy decisions relating to the responsibilities of the supplier ▪ Maintain channel of communication with the Customer Project Manager ▪ Plan the actions of those involved in the project under his responsibility
Customer Project Manager	<ul style="list-style-type: none"> ▪ Develop the installation schedule with the Supplier Project Manager ▪ Coordinate policy decisions relating to the responsibilities of the Customer ▪ Define personnel involved in the project ▪ Plan the actions of those involved in the project under his responsibility
Installer	<ul style="list-style-type: none"> ▪ Be present for the scheduled installation ▪ Wait as CIT Company withdraws cash from ATMs ▪ Wait as ATM technician prepares the ATM and installs the Note-Stop option (if appropriate) ▪ Install the Octopus[®] System and set appropriate configuration options ▪ Install CSUs in all cassettes ▪ Test & verify proper system operation ▪ Notify the customer representative that the installation is completed ▪ Complete an Installation Report
CIT (cash replenishing) Company	<ul style="list-style-type: none"> ▪ Be present for the scheduled installation ▪ Withdraw cash / cassettes from the ATM ▪ Release the electronic lock (if appropriate) ▪ Replenish money in the ATM when installation is complete
ATM Technician	<ul style="list-style-type: none"> ▪ Be present for the scheduled installation ▪ Prepare the ATM (or remove dispenser module) as required ▪ Perform a connection to the Note-Stop circuit (if appropriate) ▪ Reassemble and verify ATM operation on completion
Customer representative	<ul style="list-style-type: none"> ▪ Be present for the scheduled installation ▪ Coordinate with the Customer Project Manager as needed ▪ Assume responsible for the ATM ▪ Provide necessary conditions for installation

Appendix B – Installation Report

Date: ___/___/___

Initial Time: ___:___

Finished Time: ___:___

Customer:

Location:

ATM Make/Model:

ATM Serial No:

MCU Serial No:

<u>Check Point</u>	<u>Remarks/Comments</u>	√
iButton Reader		
AC Power & Batteries Installed		
Breach Panel: quantity and location		
Taperwire: quantity and location		
Internal Siren Installed		
Door Switch Bolt Switch Installed		
Configuration & Mode Set		
MCU PTT OK		
MCU HyperTerminal Test OK		
Arming/Disarming Key Test OK		
Note-Stop installed / tested OK		
Bank Alarm Interface Installed		
CSU quantity		
CSU PTT OK		
Ink block connector attached		
External Sticker Applied		
Internal Sticker Applied		

<u>Installer/Customer Comments</u>

Customer Representative

Company:
Name:
ID:

Installer

Company:
Name:
ID:



Appendix C – Installation Procedures

1. Determine where all system components are to be mounted:

Refer to specific mounting requirements defined below. In particular the location of the MCU must be defined so that routing of all wiring can be planned.

2. Install any optional features:

Refer to the Installation of Optional Features section below

3. Install Plug-In Power Supply:

Plug the Power Supply into an available 120 VAC Power Strip within the ATM safe. Route the low voltage wiring (with connector) to the planned MCU location.

4. Install Door and Door-Bolt Switches (as required), and other system components as described below:

Door Switch (Door-Bolt Mode only)

The Door Switch is a long throw-plunger switch. Its purpose is to detect the ATM safe door position (open / closed) The Door Switch is supplied with a mounting frame with permanent adhesive mounting tape. The Door Switch contacts are normally closed (NC) when the door is closed.



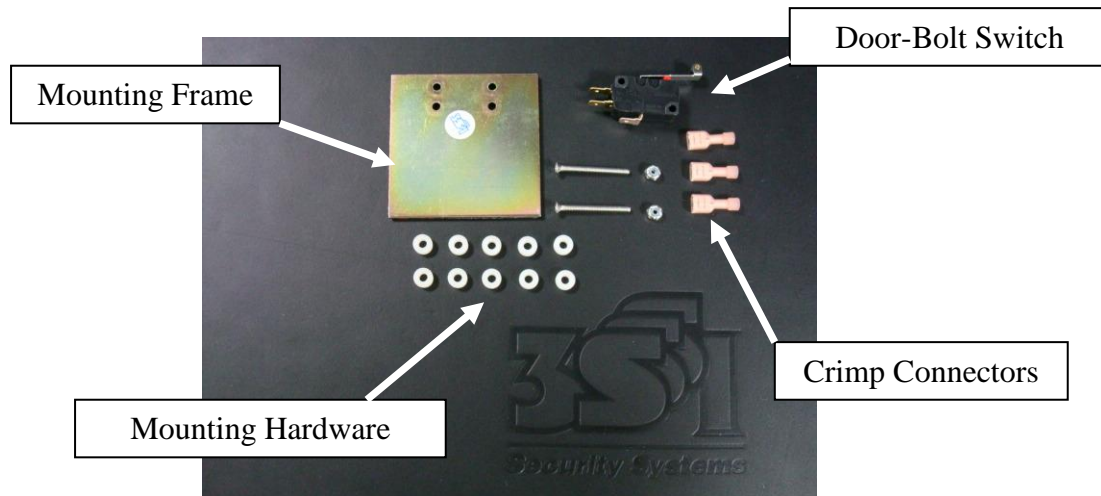
Door Switch Assembly

Mounting Notes:

- a) The door switch should be mounted away from the hinge side and cause no obstruction to the service or operation of the machine.
- b) Clean the surface where it will be mounted with the alcohol pad provided
- c) Mount the door switch $\frac{3}{4}$ inch back from the closed face of the door when shut.
- d) The door switch plunger should not impact the door where an item that moves, slides, or might otherwise cause a shearing action to the plunger.

Door-Bolt Switch (Door-Bolt Mode only)

The Door-Bolt Switch is used to detect proper authorized opening of the ATM safe lock dead-bolt. The Door-Bolt Switch contacts are normally open (NO) when the bolt is locked.



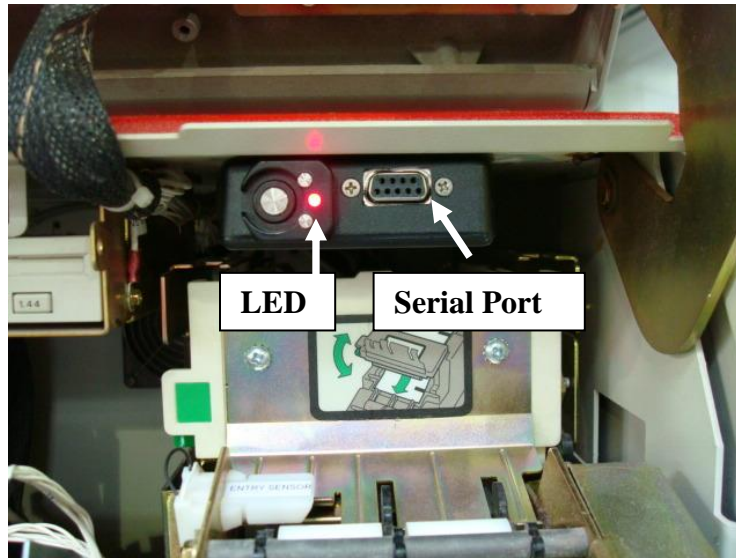
Door-Bolt Switch Assembly

Mounting Notes:

- a) The Door-Bolt switch should detect bolt movement, and if possible be wired in parallel with the electronic lock's Normally Open (NO) output.
- b) Customer should provide instructions for attaching to their lock. The contact used should be NO (normally open) when the bolt is locked and NC (normally closed) when the bolt is unlocked. This mirrors the operation of our door-bolt switch and ensures that either switch closure signals the MCU to disarm its protection.
- c) Door-Bolt switch brackets of various designs are available. Some machines may require a custom fabrication which cannot be provided at installation. If this is the case, install the system as Auto-Arming, and provide pictures, make & model to 3SI Engineering. Re-schedule door-bolt installation giving at least 2 weeks for 3SI to fabricate and provide a new bracket assembly.
- d) Route all wiring away from moving parts and secure with wire-ties.

iButton Reader

Mount the iButton Reader module in a place that is easy to access and highly visible to any ATM service technicians. It should be located inside the lockable outer ATM cabinet for security, but outside of the ATM safe. Route the iButton cable to the MCU location.



iButton Reader Mounting

MCU

Mount the MCU using hook-and-latch mounting tape, and attach all wiring.

Mounting Notes:

- a) Communication between the MCU and CSU is the best when the MCU has an unobstructed path to the CSUs. (Note: The antenna on the MCU is on the opposite side from the PTT button.)
- b) Always mount the MCU with the power plug facing up to prevent accidental unplugging.
- c) The MCU PTT button and LEDs will generally face to the rear of the ATM. They are not intended for customer use.
- d) Ideally the MCU should be mounted on the non-hinge side, forward (as close to door as possible), and low on the mounting wall. If the MCU is to be installed on the hinge side of the ATM, it should be placed as far back from the door as possible.
- e) Do not place the MCU against the rear wall of the ATM where it is obstructed by the bill picker. In 2-cassette machines this location may be acceptable, as long as the unit is mounted low on the rear wall.

ATM Warning Labels

Two sets of warning labels are provided for each ATM installation. The external label is applied to the ATM exterior, and indicates to ATM users that the ATM is protected with the Octopus[®] ATM Defense System. The internal labels are applied to the interior of the ATM cabinet and on all Cassettes, and indicate to maintenance personnel that an Octopus[®] System is installed.



External Label



Internal Labels

CSU Installations

Install a CSU in each of the currency cassettes in accordance with the 3SI Cassette Installation Instructions for the specific make and model of cassette. (Refer to separate 3SI procedures.)

NOTE - Important: The CSU Ink Block connector must not be connected until the Octopus[®] System installation is complete, and all tests have been run.

Appendix D – Managing iButton Keys

The Octopus[®] system uses 3 distinct iButton keys: a blue iButton key, a black iButton key, and a white iButton key. The system is shipped with 2 blue iButton keys configured to work only with the supplied MCU. The blue iButton keys are used for turning the system on and off.

The black and white iButton keys are used only by 3SI service personnel for key management and replacement. Up to 3 blue keys can be stored / registered in the MCU. Multiple MCUs can also have the same keys stored to them if required.

If no keys are stored to an MCU, any blue key will work.

Training Blue iButton Keys

To train up to 3 blue iButton keys to an MCU, follow these directions:

1. Place the black iButton key on the iButton reader of the MCU to open the session and train new keys. The LED on the iButton reader should begin blinking green.
2. Place the black iButton key on the iButton reader. The LED on the iButton reader should go to solid green.
3. Place at least 2 and up to 3 blue iButton keys on the reader, one at a time.
4. The LED should flash once for 1 key, twice for 2 keys and solid green for 3 keys.
5. To end the session, place the black iButton key on the iButton reader, after at least 2 blue keys have been trained.
6. If the storage is successful, the LED will alternate red/green for approximately 2 seconds, then go off.
7. If the storage is unsuccessful, the unit will timeout and blink the LED red for 2 seconds.

Erasing Blue iButton Keys

To erase stored blue iButton keys:

1. Place the black iButton key on the iButton reader to open the session and erase keys. The LED on the iButton reader should begin blinking green.
2. Place the white iButton key on the iButton reader to which the blue keys are trained.
3. If the erase is successful, the LED will alternate red/green for approximately 2 seconds before extinguishing.
4. If the storage is unsuccessful, the unit will timeout and blink the LED red for 2 seconds.

Appendix E – Serial Communications Access

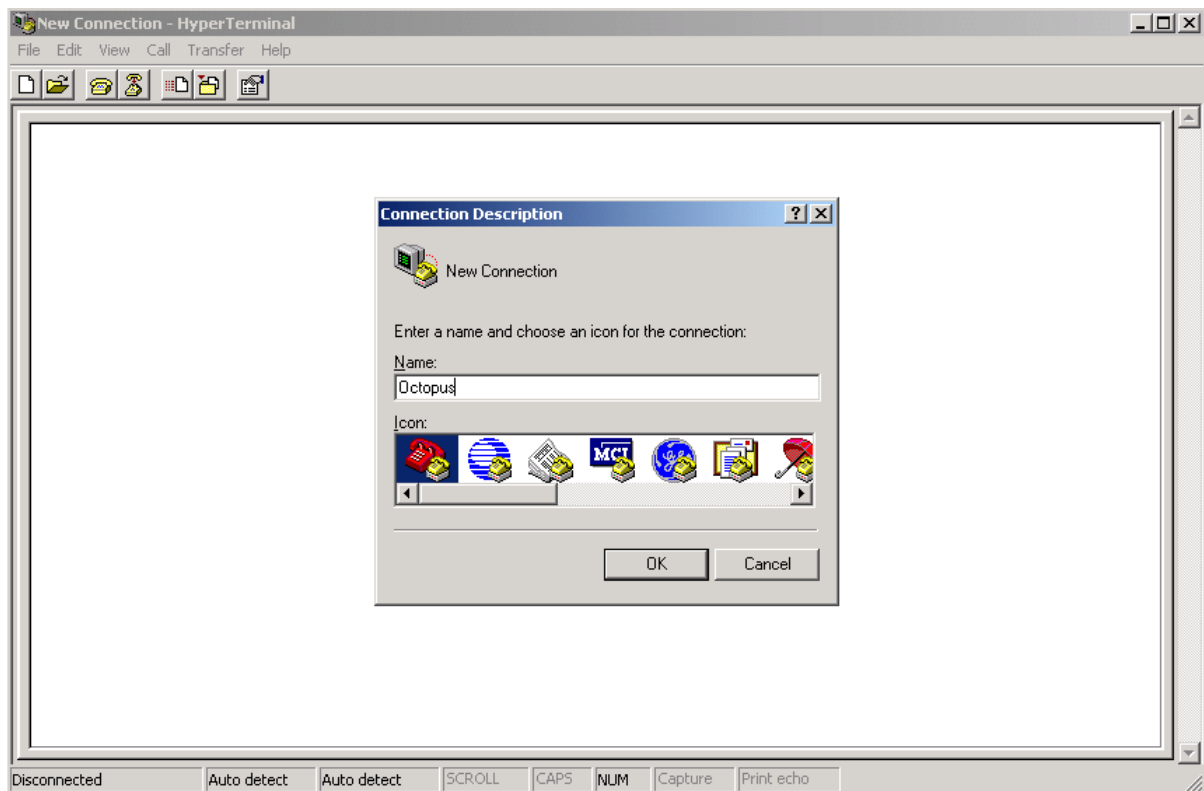
If the system is Disabled (iButton LED off), serial communications can be established with the MCU. Any ASCII serial communication tool can be connected. Communication parameters are 9600 baud, 1 stop bit, no flow control. The serial interface provides:

- Retrieval of the internal system event log.
- Ability to enable a system without a preconfigured iButton Key.
- Ability to upgrade the system firmware without system removal.
- Various test procedures for installation personnel.

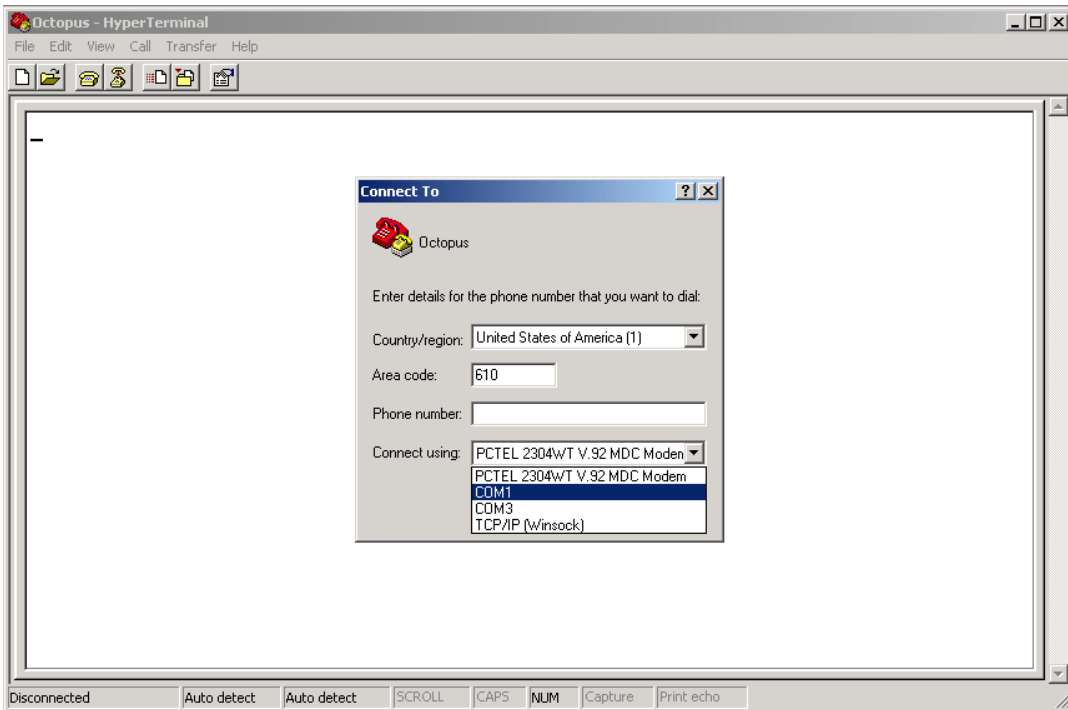
Needed: RS232 cable, laptop computer, valid blue iButton key

Setting up Initial Serial Communications

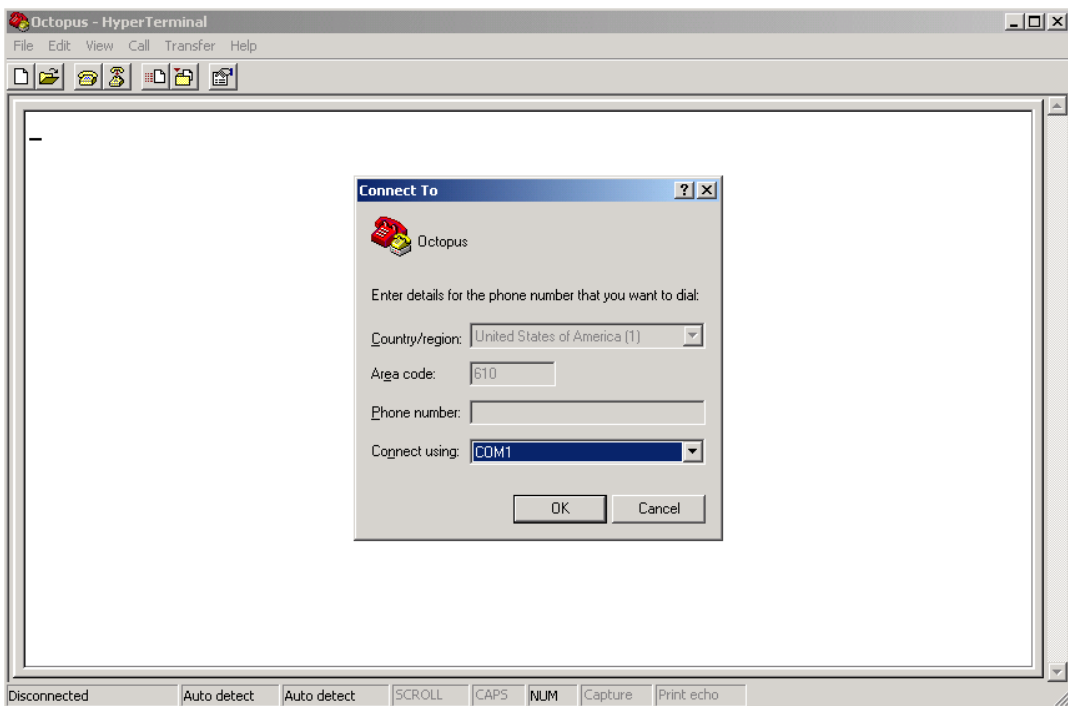
1. On your desktop, choose Start Menu > Programs > Accessories > Communications > HyperTerminal.
2. When prompted with the Connection Description box, name the new connection “Octopus” and click Ok.



3. When prompted with the Connect To box, go to “Connect Using” and choose **COM1**. This tells the computer which hardware interface to use. COM1 is the standard.

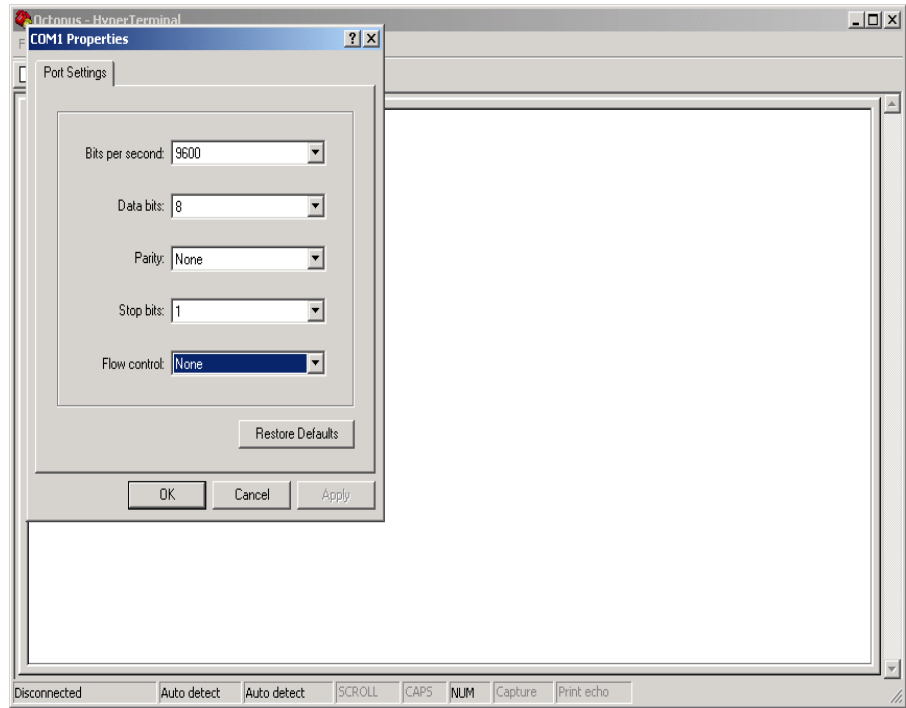


4. After choosing COM1, click Ok.

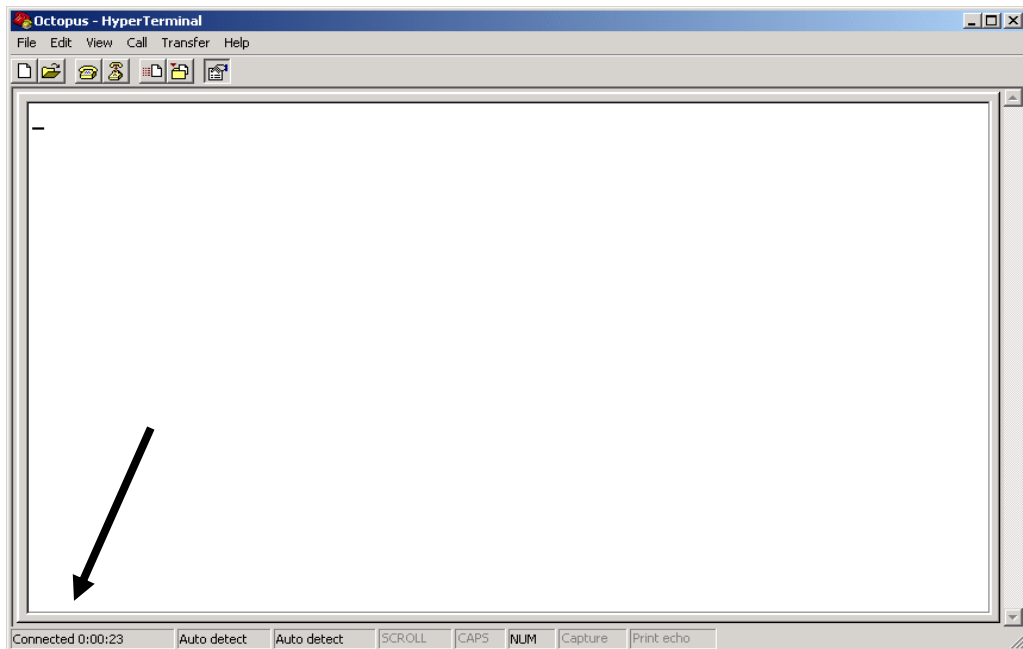


5. When prompted with the Port Settings box, enter the following information, then click OK:

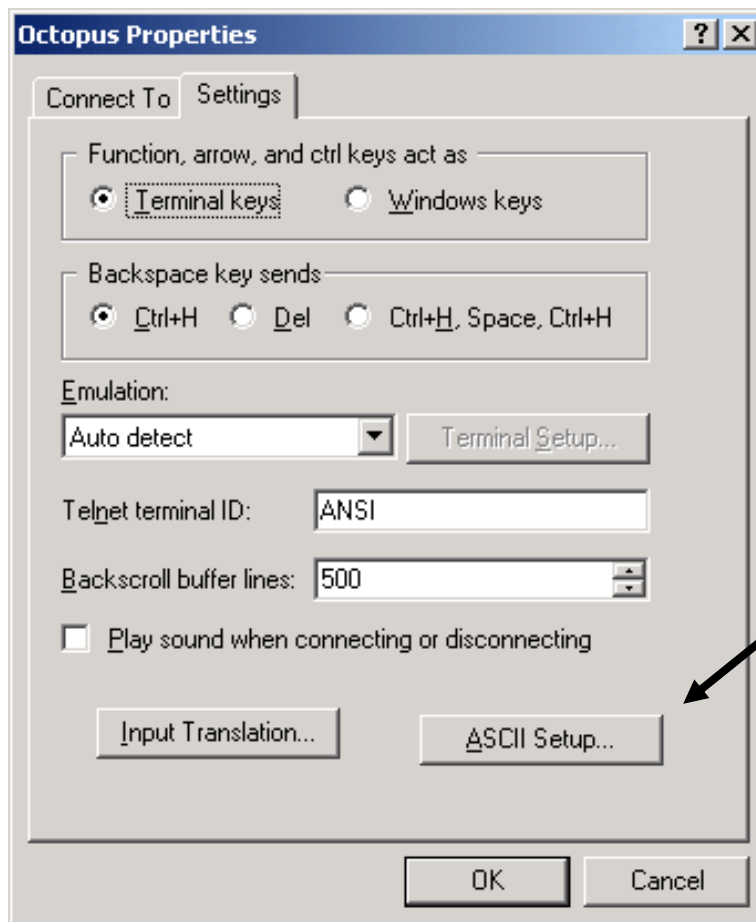
- Bits per second: 9600
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None



6. Successful communication is indicated in the bottom left-hand corner of the screen where it will say “Connected”, followed by the elapsed time of the connection.

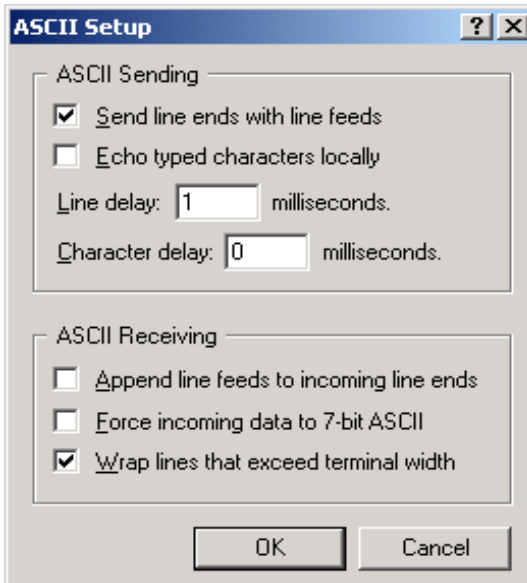


7. Go to File > Properties, choose the Settings tab, then click the ASCII Setup button.



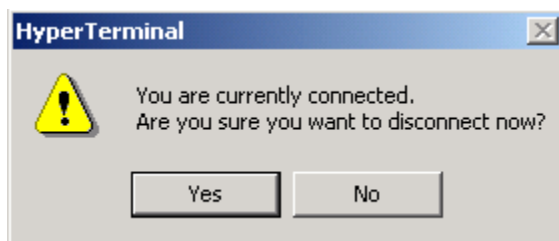
8. In the ASCII Setup box, change the following:

- Check “Send line ends with line feeds”
- Change the Line Delay to 1 millisecond
- Click Ok.

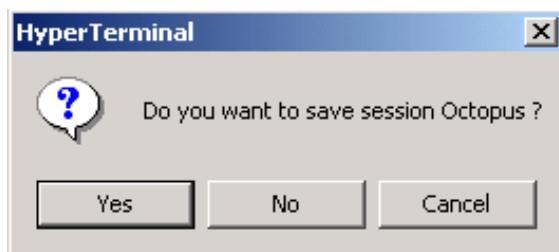


9. Click Ok on Settings to close the window.

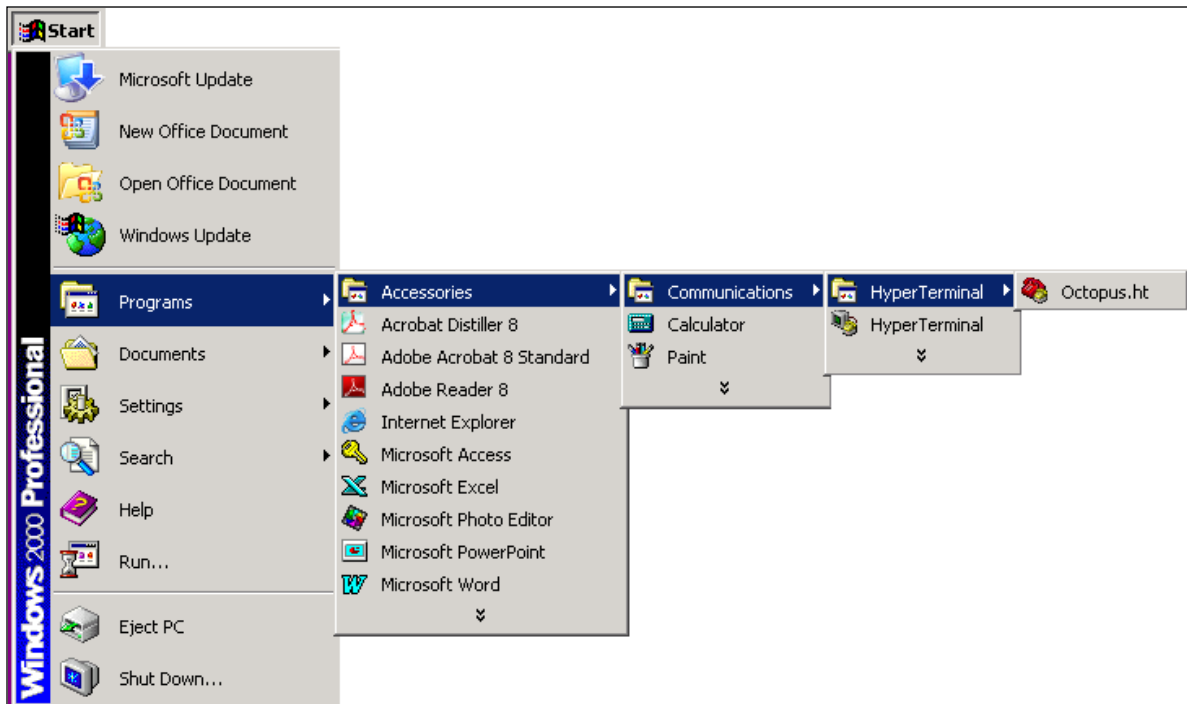
10. Close the HyperTerminal window. You will get a dialogue box asking if you are sure you want to disconnect. Click Yes.



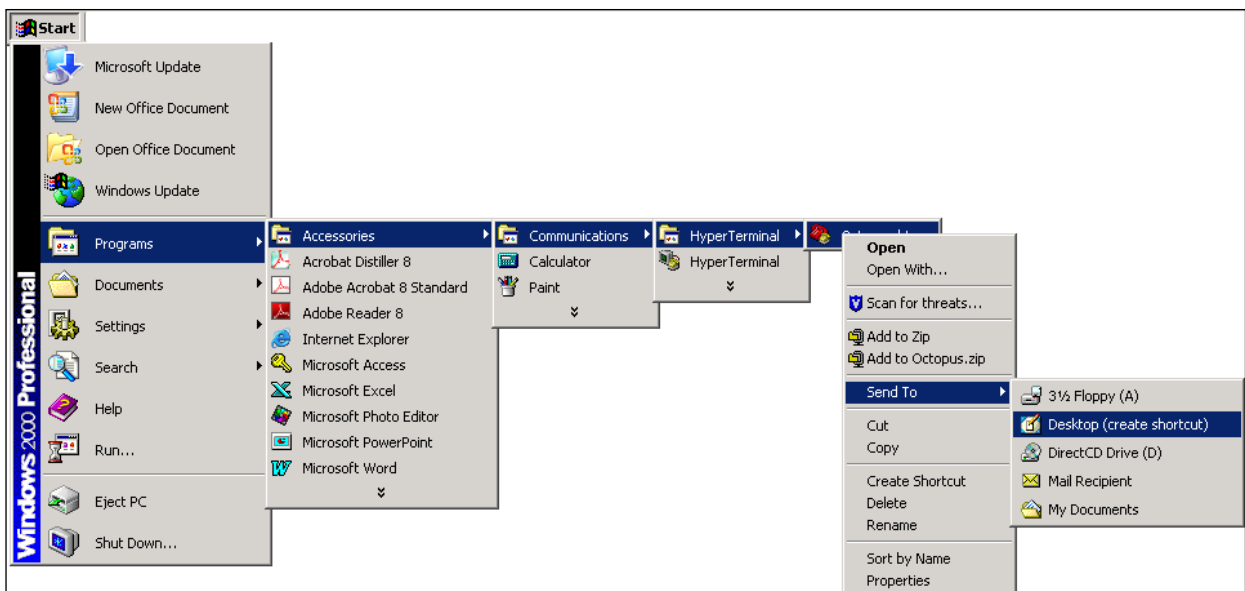
11. You will get a dialogue box that asks if you want to save session. Click Yes.



After saving the HyperTerminal connection “Octopus”, the connection will always be in HyperTerminal folder.



To save it on the desktop for easy future access, right click on the file and choose Send to > Desktop (create shortcut). An icon will appear on the desktop.

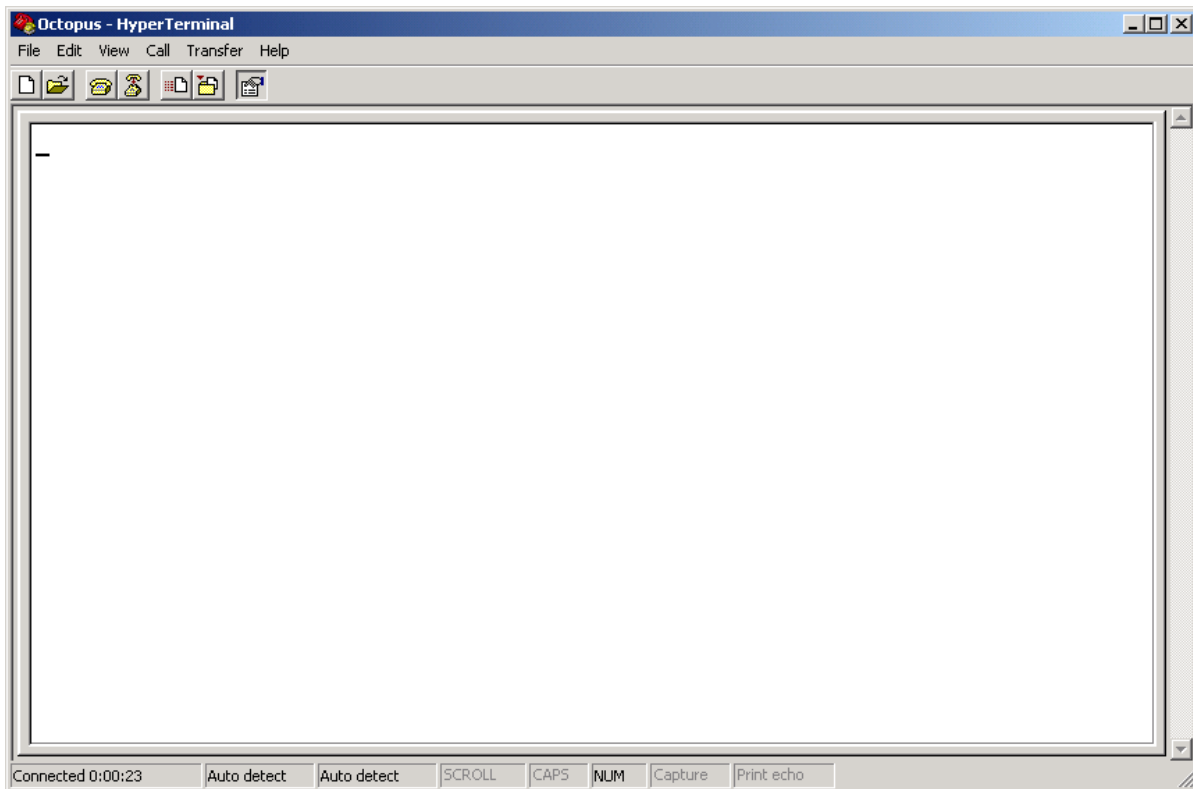


Accessing Serial Communications and Using the Menu

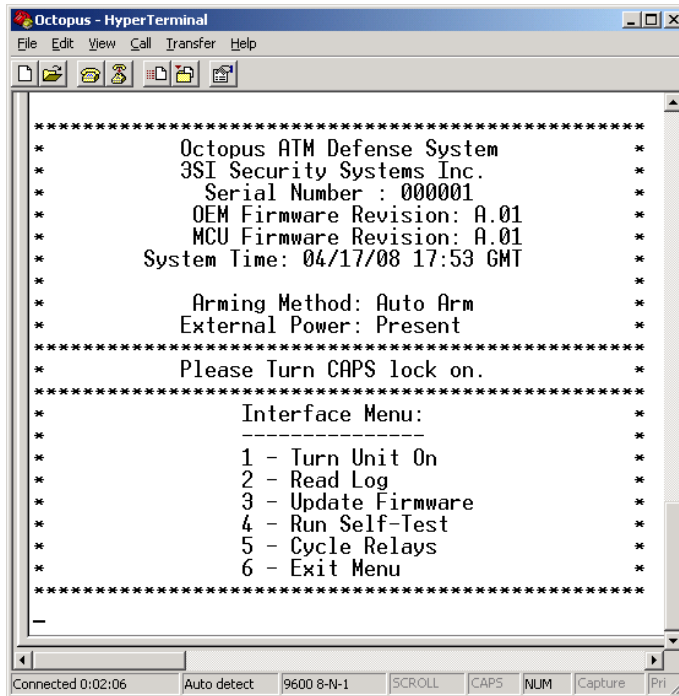
To initiate serial communications with the Octopus[®] system, follow these instructions.

Note: The Octopus[®] system can only communicate with a computer when the system is in the Disabled State. If the system is Armed, it must first be turned off with a blue iButton key.

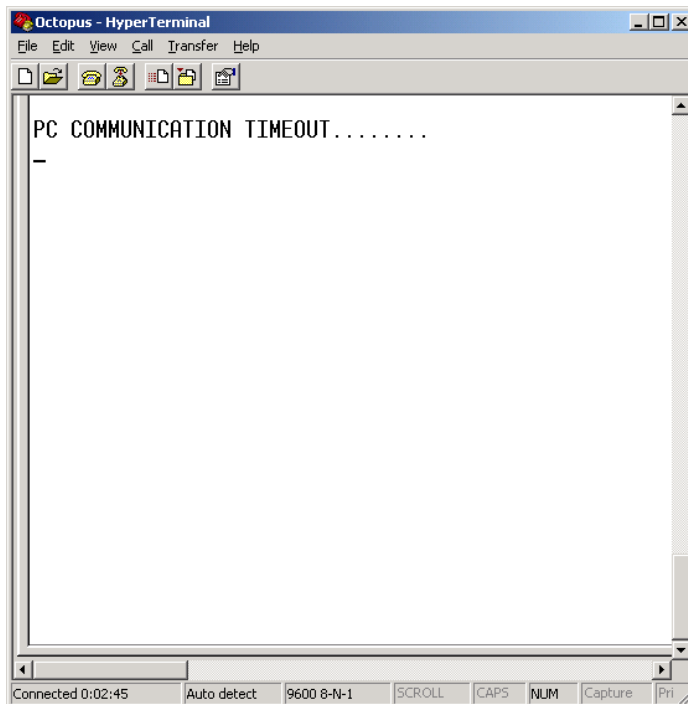
1. Plug in an RS232 cable to the mating RS232 connector on the Octopus[®] iButton reader.
2. Open the saved HyperTerminal connection by clicking on the previously created desktop shortcut or by going to Start Menu > Programs > Accessories > Communications > HyperTerminal > Octopus.
3. Once the session is started, you will see the following screen.



4. Press spacebar to access the main menu which will look like this:



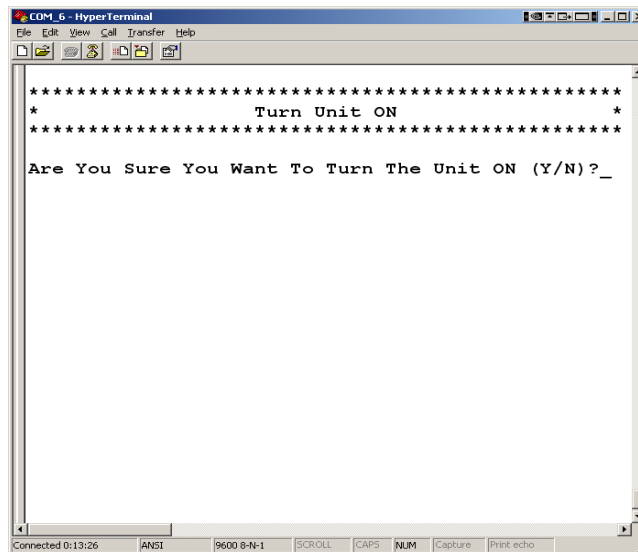
5. If no key is pressed for 1 minute, you will receive the PC Communication Timeout screen. Press spacebar again to return to main menu.



Navigating the Main Menu (Note: Caps lock must be ON)

1. Turn Unit On

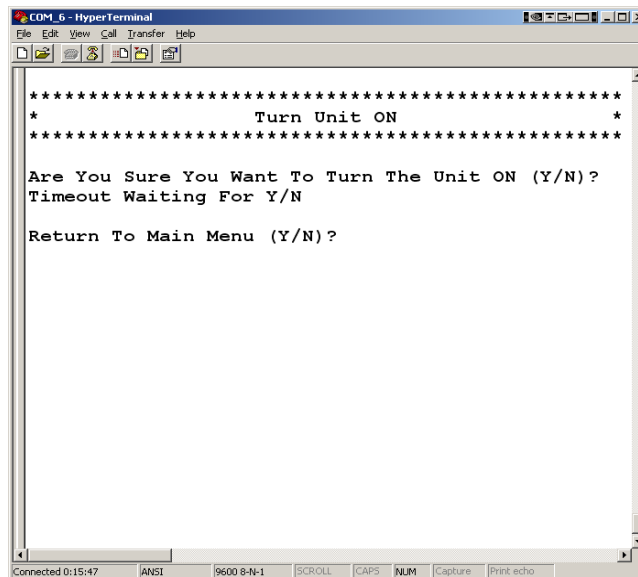
- a) Press 1 on the keyboard
- b) You will receive the following warning screen because you can *only* turn the unit ON with serial communications—if you do not have a blue iButton key, you *cannot* turn the system OFF once it is On.



```
COM_6 - HyperTerminal
File Edit View Call Transfer Help
*****
*           Turn Unit ON           *
*****
Are You Sure You Want To Turn The Unit ON (Y/N)?_
```

Connected 0:13:26 ANSI 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

- c) After you type “Y,” the unit is on but won’t go into Armed state yet. You must exit this menu by pressing “Y,” then type “6” to exit the main menu.



```
COM_6 - HyperTerminal
File Edit View Call Transfer Help
*****
*           Turn Unit ON           *
*****
Are You Sure You Want To Turn The Unit ON (Y/N)?
Timeout Waiting For Y/N

Return To Main Menu (Y/N)?
```

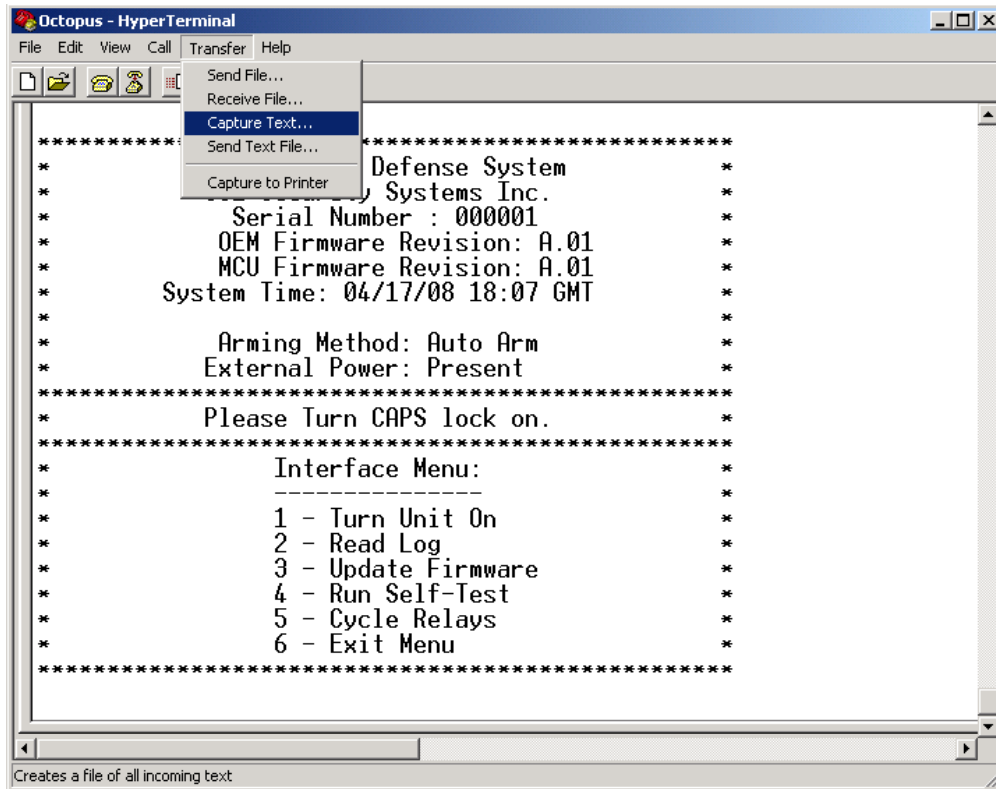
Connected 0:15:47 ANSI 9600 8-N-1 SCROLL CAPS NUM Capture Print echo

Note: Remember that there is no way to get back once you exit the main menu and enter the Armed State, unless you have a key.

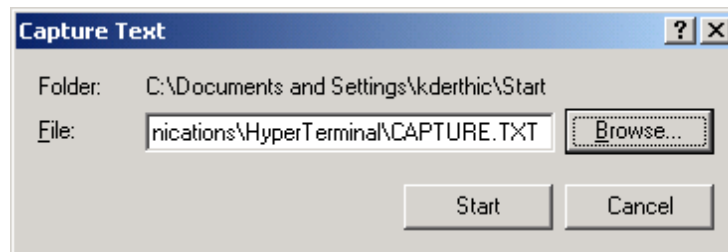
2. Capture Text File and Read Log

Note: Before you choose Read Log, you must first capture the session to text file. That way, if there is a problem you want to report, you have a copy of the session to send to 3SI.

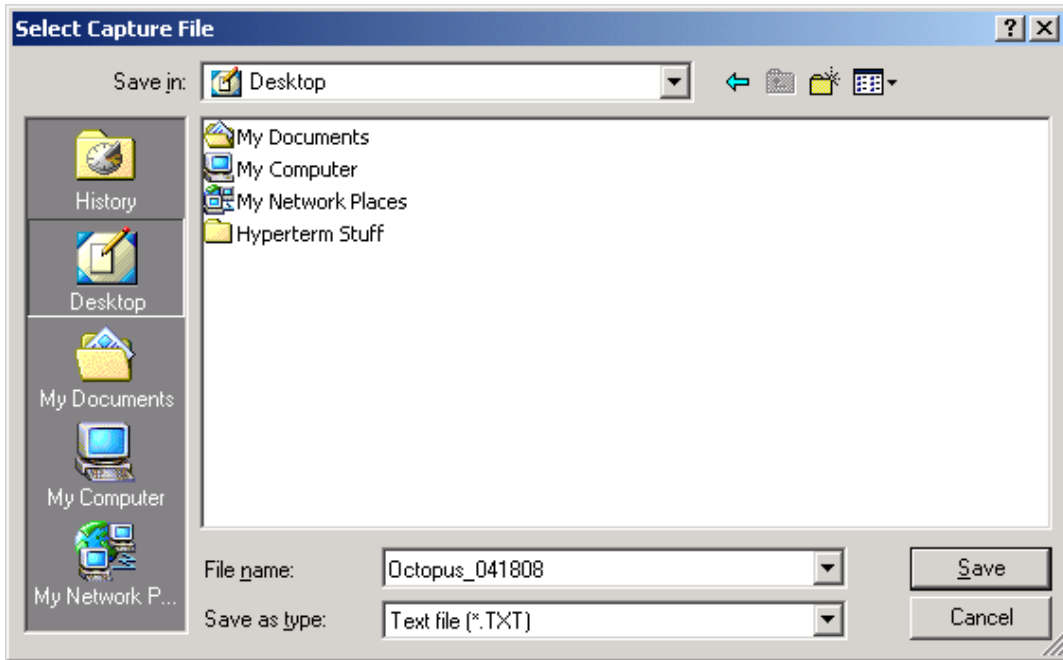
- a) At the top of the window, Choose Transfer > Capture text.



- b) Browse to the folder where you want to save text file by clicking Browse.



c) Name the file Octopus_”date” and click Save. Then click Start.



d) After you save the text file, type “2” to read the log:

Serial # of each key. If all 0s, any 3SI key will work.

Cause of last activation.

Cause of last Arming.

Cause of last Disarming.

Last 16 events. Next 14 are on following page (press Y to continue).

```

KEYS (1) 000000000000 (2) 000000000000 (3) 000000000000
LAST ACTIVATION EVENT 04/17/08 16:05 QA TILT VIOLATION
LAST ARMING EVENT 04/17/08 17:58 ARMING DELAY EXPIRED
LAST DISARM EVENT 04/17/08 17:58 BLUE KEY GEN

04/17/08 17:58 BLUE KEY GEN DISABLED 00
04/17/08 17:58 ERROR BREACH PRE-ARMED 00
04/17/08 17:58 PC ACCESS ENABLED 00
04/17/08 17:58 PC ACCESS ENABLED 00
04/17/08 17:58 PC ACCESS ENABLED 00
04/17/08 17:58 BLUE KEY GEN DISABLED 00
04/17/08 17:58 ARMING DELAY EXPIRED ARMED 00
04/17/08 17:58 ERROR BREACH PRE-ARMED 00
04/17/08 17:58 PC ACCESS ENABLED 00
04/17/08 17:58 PC ACCESS ENABLED 00
04/17/08 17:58 PC ACCESS ENABLED 00
04/17/08 17:57 BLUE KEY GEN DISABLED 00
04/17/08 17:57 ERROR BREACH PRE-ARMED 00
04/17/08 16:06 QA BLUE KEY GEN DISABLED 81
04/17/08 16:05 QA TILT VIOLATION ACTIVATION 81

Continue ?_
  
```

The log readout shows the last 30 events, date, time (in GMT), what the event was, what state the unit was in, and the status of dip-switches (whether dip-switches were on or off).

The 30 events are provided on two pages: 16 events on the first page, 14 events on second page. To continue and access the second page, type “Y”.

```

Octopus - HyperTerminal
File Edit View Call Transfer Help
04/17/08 17:58 PC ACCESS          ENABLED      00
04/17/08 17:58 PC ACCESS          ENABLED      00
04/17/08 17:57 BLUE KEY GEN       DISABLED     00
04/17/08 17:57 ERROR BREACH      PRE-ARMED   00
04/17/08 16:06 QA BLUE KEY GEN   DISABLED     81
04/17/08 16:05 QA TILT VIOLATION ACTIVATION   81

Continue ?
04/17/08 16:05 QA ARMING DELAY EXPIRED ARMED        81
04/17/08 16:04 QA INCORRECT CLOSURE SEQ  ENABLED      81
04/17/08 16:04 QA BLUE KEY GEN       ENABLED      81
04/17/08 16:04 BLUE KEY GEN         DISABLED     00
04/17/08 16:04 BREACH OPENED       ACTIVATION   00
04/17/08 16:04 ARMING DELAY EXPIRED ARMED        00
04/17/08 16:04 BLUE KEY GEN         ENABLED      00
04/17/08 16:03 BLUE KEY GEN         DISABLED     00
04/17/08 16:03 ARMING DELAY EXPIRED ARMED        00
04/17/08 16:03 BLUE KEY GEN         ENABLED      00
04/17/08 15:45 BREACH OPENED       ACTIVATION   00
04/17/08 15:42 ARMING DELAY EXPIRED ARMED        00
04/17/08 15:42 BLUE KEY GEN         ENABLED      00
04/17/08 15:42 BLUE KEY GEN         DISABLED     00

Return To Main Menu (Y/N)?

Connected 0:15:10  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo

```

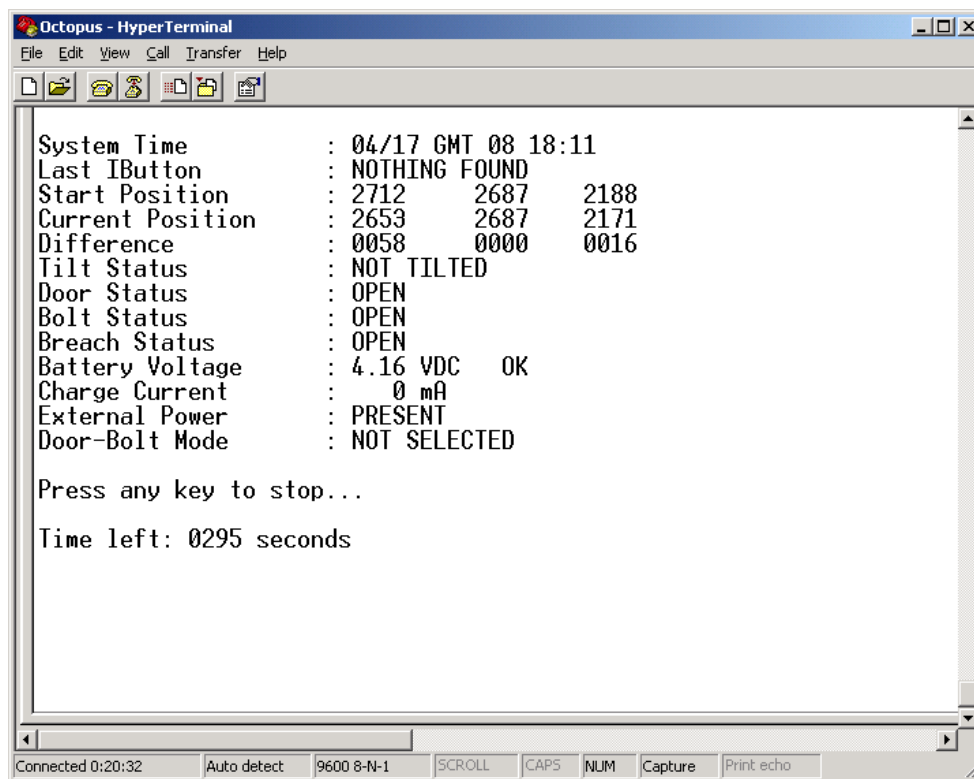
3. Update Firmware

Update Firmware should not be accessed without first contacting 3SI.



4. Run Self-Test

Typing “4” to run the self-test will produce the following screen:



```
Octopus - HyperTerminal
File Edit View Call Transfer Help

System Time      : 04/17 GMT 08 18:11
Last IButton     : NOTHING FOUND
Start Position   : 2712    2687    2188
Current Position : 2653    2687    2171
Difference       : 0058    0000    0016
Tilt Status      : NOT TILTED
Door Status      : OPEN
Bolt Status      : OPEN
Breach Status    : OPEN
Battery Voltage  : 4.16 VDC   OK
Charge Current   : 0 mA
External Power   : PRESENT
Door-Bolt Mode   : NOT SELECTED

Press any key to stop...

Time left: 0295 seconds

Connected 0:20:32  Auto detect  9600 8-N-1  SCROLL  CAPS  NUM  Capture  Print echo
```

Each line provides system status information:

System Time: Provides current time in GMT with a real-time clock.

Last iButton: Provides the serial number of the last iButton Key used. If, during self-test you key an iButton, the screen will provide the serial number and color of the button. Use this to verify that the iButton Key is valid.

Start Position: Provides analog-to-digital converter readings of the accelerometer XYZ axes at startup that are used as the reference for detecting tilt.

Current Position: Provides analog-to-digital converter readings of the accelerometer XYZ axes in their current position.

Difference: Shows the difference between start position and current position. You can slowly move the unit around and watch the current position change. Watch Difference to confirm the accelerometer is working.

Tilt Status: Shows whether unit is tilted or not. Tilt Status changes as you rotate the MCU.

Door Status: Shows whether the door is open or closed.

Bolt Status: Shows whether the bolt is open or closed.

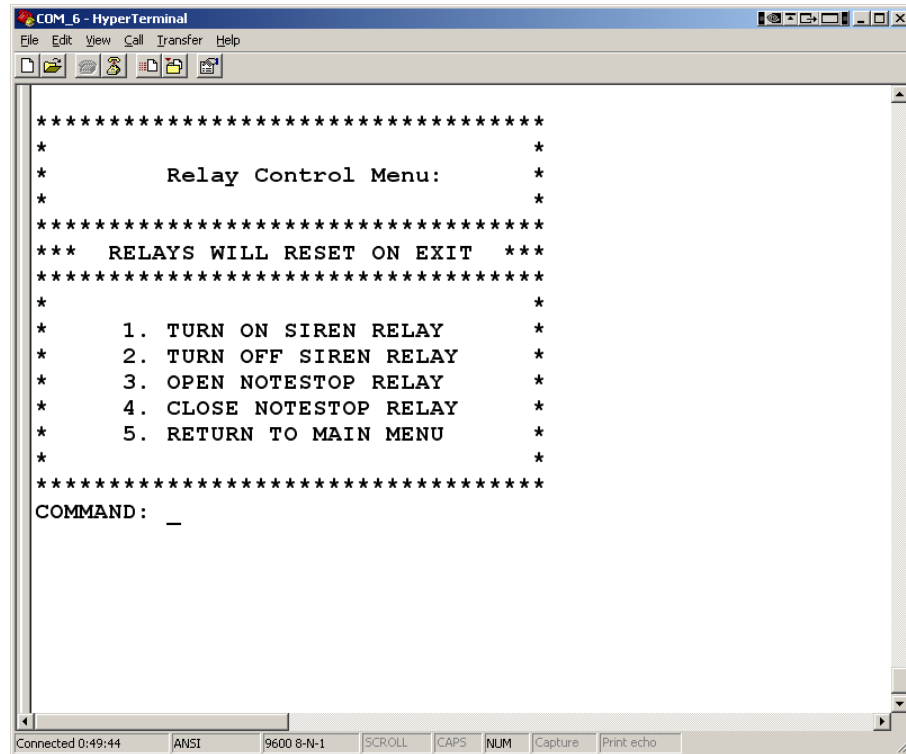
Breach Status: Shows whether the breach panel is open or closed.

Battery Voltage: Provides the current battery voltage and whether the voltage is strong enough for operation.

- Charge Current:** Shows whether the battery is being charged. If the number is greater than 100 mA, the unit is being charged.
- External Power:** Shows whether external power is present or not.
- Door-Bolt Mode:** Shows whether Door-Bolt Mode is selected or not.
- Time Left:** Shows the self-test time remaining. Self test will run continuously for 5 minutes (300 seconds) or until a key is pressed to exit.

5. *Relay Control Menu*

- a) The Relay Control Menu allows you to test the MCU relays, which control external devices (Internal Siren, Note-Stop, etc.). Once in the Relay Control Menu, type the number you want. (You do not have to press enter after the number.) Type 5 to exit.



6. *Exit Menu*

Type “6” to exit the main menu. If you want to Arm the system, you *must* exit the menu and then key it on with a blue iButton key.

Appendix F – Optional Features

Bank Alarm Interface

The Bank Alarm Interface feature enables the MCU to notify the bank's alarm system that the ATM has been attacked. A set of normally closed (NC) contacts are provided for this purpose. Connection is made via either J14 or J15 using a standard RJ-11 connector.

Internal Siren Module

The Internal Siren Module is a self-powered 128 dB audio siren. The siren will alert onlookers and possible witnesses that the ATM has been attacked. Once activated, the siren will require battery replacement. The siren uses a standard 9V alkaline battery.



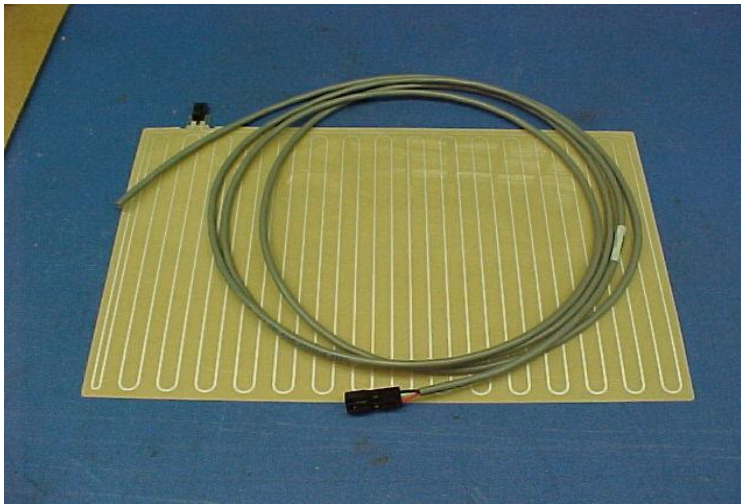
Internal Siren Module

Breach Sensor

The Breach Sensor is used to detect drill or torch attacks on the ATM safe walls. The circuit is normally closed until the sensor is penetrated or broken. The sensor is wired to J31 pin 1 and J10 pin 2. The normally closed circuit is made up of a Mesh Panel (for wide areas), and flat Taperwire (for small spot protection).

Mesh Panel

The Mesh Panel is an adhesive panel whose purpose is to provide penetration protection for ATM safe walls. The customer should provide details as to the most likely methods of attack and desired protection areas.



Mesh Panel

Taperwire

The Taperwire is an adhesive-backed flat wire. Its purpose is to provide spot protection for along the ATM safe walls. The customer should provide details as to the most likely methods of attack and desired protection areas.



Taperwire

Note-Stop

The Note-Stop option adds the capability to shut down the ATM in the event of an attack (so that it will not dispense money). Installation of the Note-Stop requires interruption of the ATM internal power, and requires coordination with the ATM manufacturer.