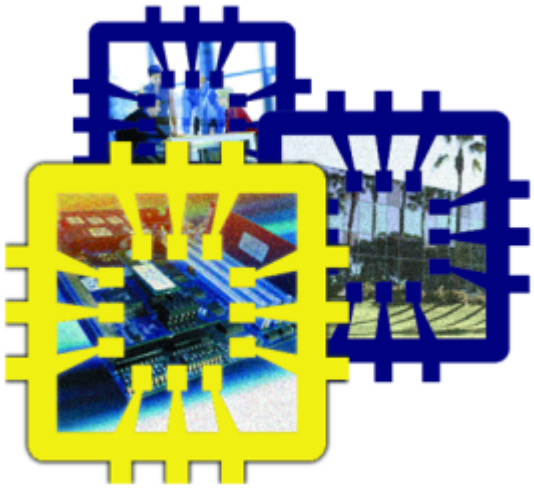
AAN-4 Hardware Manual

Revision Date: 25 AUG 2010



AAN-4 Hardware Manual

Advanced Electronic Controller For Apollo Access Control Systems

---

by Apollo Security Inc.

IMPORTANT INFORMATION

W A R N I N G
HIGH VOLTAGE, AC MAIN POWER SHOULD ONLY BE CONNECTED BY QUALIFIED, LICENSED ELECTRICIANS. ALL APPLICABLE LAWS AND CODES MUST BE FOLLOWED. IF THIS PRECAUTION IS NOT OBSERVED, PERSONAL INJURY OR DEATH COULD OCCUR

Power should not be applied to the system until after the installation has been completed. If this precaution is not observed, personal injury or death could occur, and the equipment could be damaged beyond repair.
-Verify that the external circuit breaker which supplies power to the device power supply is turned off prior to installation.
-Verify that the output voltage of the power supply is within specifications prior to connection to the device.

C A U T I O N
Several important procedures should be followed to prevent electro-static discharge (ESD) damage to sensitive CMOS integrated circuits and modules.

-All transport of electronic components, including completed reader assemblies, should be in static shield packaging and containers.
-Handle all ESD sensitive components at an approved static controlled work station. These work stations consist of a desk mat, floor mat and a ESD wrist strap. Work stations are available from various vendors including the 3M company.

FCC Compliance Statement
This device complies with Part 15 of FCC Rules. Operation is subject to the following two conditions:

1.This device may not cause harmful interference, and
2.This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense. The user is advised that any equipment changes or modifications not expressly approved by the party responsible for compliance would void the compliance to FCC regulations and therefore, the user's authority to operate the equipment.

Table of Contents

Part I Introduction 2

1 Overview 2
2 General Features 2
3 Modes Of Operation 2
4 Programming Host 3

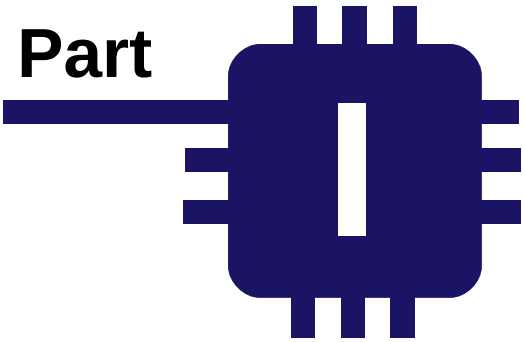
Part II Hardware Layout 6

1 Terminal Connectors 6
2 DIP Switches 10
DIP Switch Tables 10
DIP Switch Function 11
3 Connectors 11
Device Port Communication Driver Socket 12
Additional Connectors 12
4 LEDs 12
Start Up Mode 12
Normal Operation 13
5 Firmware 13
6 Memory Backup 13
7 Additional Installation Information 14
Mounting Holes 14

Part III System Wiring 17

1 Power 17
2 Grounding 17
DC Ground 17
RS-485 Signal Ground (SG) 17
Safety (Earth) Ground 18
Grounding System 18
Grounding Potential Difference Checks Before Connecting 18
3 Host Communication Connection 18
Serial 19
Network 20
ENI-100 21
Introduction 21
Hardware Layout 21
Connectors 21
TTL Serial Connector 21
RJ-45 Jack 21
Communication Configuration 22
4 Card Reader Wiring 24

5 Reader Input Wiring 26
Input Supervision (Overview) 26
Door Contact Input (Door Position Switch) 27
Exit Pushbutton Input (Request To Exit, REX) 28
Auxiliary Alarm Inputs 28
6 Output Relay Wiring 28
Strike Wiring, General 29
Strike Suppression Installation 29
Strike Wiring, Internal Relay 30
ADA External High Security Relays 32
Strike Wiring, External ADA-10/11, High Security Relay 32
Additional Output Relay Wiring 33
ADA DIP Switches/Jumpers 34
7 General Alarm Inputs 35
Cabinet Tamper 35
Part IV Software Configuration Utilities 37
1 ENI-100 IP Programming 37
InitAAN 38
Web Page 41
Telnet 44
Part V Troubleshooting 48
1 Communications 48
2 Reader / Keypad 48
3 Input Zones 48
4 Output relays 48
Part VI Specifications 50
Part VII Supplemental Figures 52
Part VIII Table of Figures 60
Part IX Revision History 62
Index 63



Introduction

APOLLO
intelligent security solutions

1 Introduction

An access control system provides a means to replace traditional key and lock systems, which are easy to defeat because of the ease of copying of keys and use by unauthorized personnel. With electronic access control, the exact areas a person is able to access as well as during what time is configurable through a central control system. In addition to the power of greater control, a historical record is maintained which is useful in the case of a system security breach or for other purposes including calculating work time and facility use costing.

1.1 Overview

The AAN-4 Access and Alarm Network Controller is a self-contained controller for four card readers and door hardware as well as additional alarm inputs and outputs. Typical use of the is the control of site access by control of door locking devices associated with card readers and PIN keypads and maintaining logs of this access for later reporting.

The AAN-4 works through connection to a host programming device (PC computer with a database interface application), which defines configuration for the four built-in reader interfaces. The connections between the AAN-4 and host can be made via Ethernet TCP/IP (AAN-4N) or RS-232 or RS-485 serial connection (AAN-4S).

By supporting both centralized and distributed database operation, once the AAN-4 controller has been programmed from the host device, it will work independently and only require connection to the host for live event monitoring and reporting of events to the database. All the necessary information to carry out access decisions and other response functions of the system is stored within the AAN-4's internal memory and does not rely on a constant connection to the host computer.

The AAN-4 provides interface connections for a variety of card reader technologies, including proximity, biometric, bar code, and infrared readers. Any card reader with standard Wiegand or mag stripe output can be connected to the AAN-4. Provided for each of the four readers are exit push button, door contact and other general purpose inputs as well as are on-board strike relays and additional general purpose relay outputs. The AAN-4 communicates with host software to obtain configuration and report system events. A downloadable card database of up to 20,000 cardholders and storage of up to 7000 events allows the AAN-4 to work independently after initial programming.

1.2 General Features

- Supports 4 readers, keypads or reader/keypad combinations for 4 door control
- Full Stand Alone Operation with Local database of 20,000 cards or 7,000 events
- Multiple Card Formats
- Up to 8 Facility Codes
- 8 Relay Outputs (4 Door strike, 4 Auxiliary)
- Control of up to 16 ADA-10/11 High Security Relay Output Modules
- Interchangeable TCP/IP, RS-485 or RS-232 interfaces
- 12 Inputs (4 Door Contact, 4 Exit Pushbutton, 4 Auxiliary)
- Field-Replaceable plug-in communication drivers
- Real Time Clock
- Firmware stored in flash memory for easy upgrade
- Surface-mount manufacturing technology

1.3 Modes Of Operation

To establish operating configuration, the AAN-4 interface requires connection to a host programming device which contains a software database interface program. Configuration options including cardholders are stored in a central database and then transmitted via a proprietary encrypted protocol to the AAN-4 controller. The AAN-4 controller will communicate with the host to download the following configuration information:

- Card Reader Data Output Format: Wiegand or Mag Stripe
- Strike Time—The time duration that the strike relay will be energized for in the case of an access grant
- Held Open Time—After an access grant and a subsequent opening of the door contact, the time in which the door contact must be closed before an alarm state is reported
- Initial Reader Mode—The access mode in which the reader will function upon powering up or when communication has been interrupted between the AAN-4 and host. The following modes are supported:

  - Card Only—An access request is made by presenting a card to the reader. The data is verified against the AAN-4 database to ensure that the card has a valid Facility Code and Card Number.
  - Card or PIN—Access requests are made either by presenting a card or by keying in a PIN (Personal Identification Number) on a keypad. A card entry is process as in Card Only access mode.
  - Card & PIN—A card must be read to start the access request. If the card is valid, the user is prompted to enter the corresponding PIN. The request is granted only if the card and PIN match.
  - Locked—No access granted. Reader ignores all cards and PIN entries.
  - Unlocked—Door strike is continuously energized and the door contact input is not monitored. Access is not controlled.
  - Facility Code—The entire card contents are read by the AAN-4, but only the Facility Code is checked, and if it matches a Facility Code downloaded from the programming host, access is granted.

1.4 Programming Host

To establish operating configuration and to report events, the AAN-4 controller requires connection to a software database interface program. Configuration options including cardholders are stored in a central database and then transmitted via a proprietary encrypted protocol to the AAN-4. Once programmed, the AAN-4 will continue to function without connection to the host. A record of all actions that happen while there is no connection is stored in the memory of the AAN (limited by the capacity of the memory) for reporting at a later time when connection with the host has been re-established.

Apollo has designed the APACS software system to provide the closest integration possible to take full advantage of the features of the AAN-4 controller. Full documentation on configuring the options of the AAN-4 with APACS is contained in the documentation provided with the software.

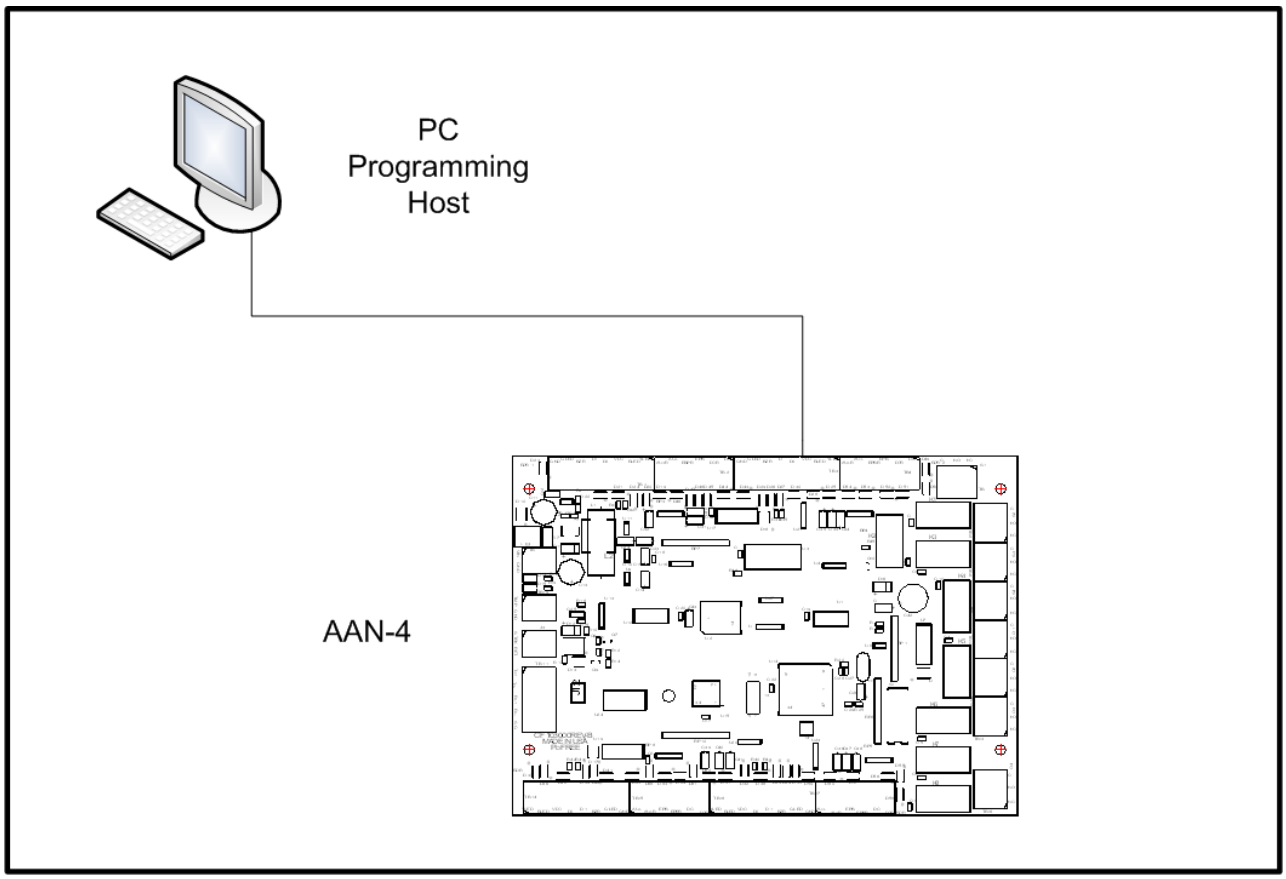
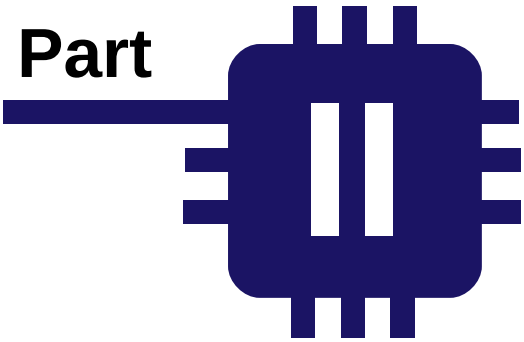


Figure 1.3 Programming Host Logical Diagram. Typical System Layout with RS-485 Connections. Several AAN-4 panels can be connected to one host on an RS-485 line using different device addresses. Field devices on the same line must also have unique addresses.



Hardware Layout

APOLLO
intelligent security solutions

2 Hardware Layout

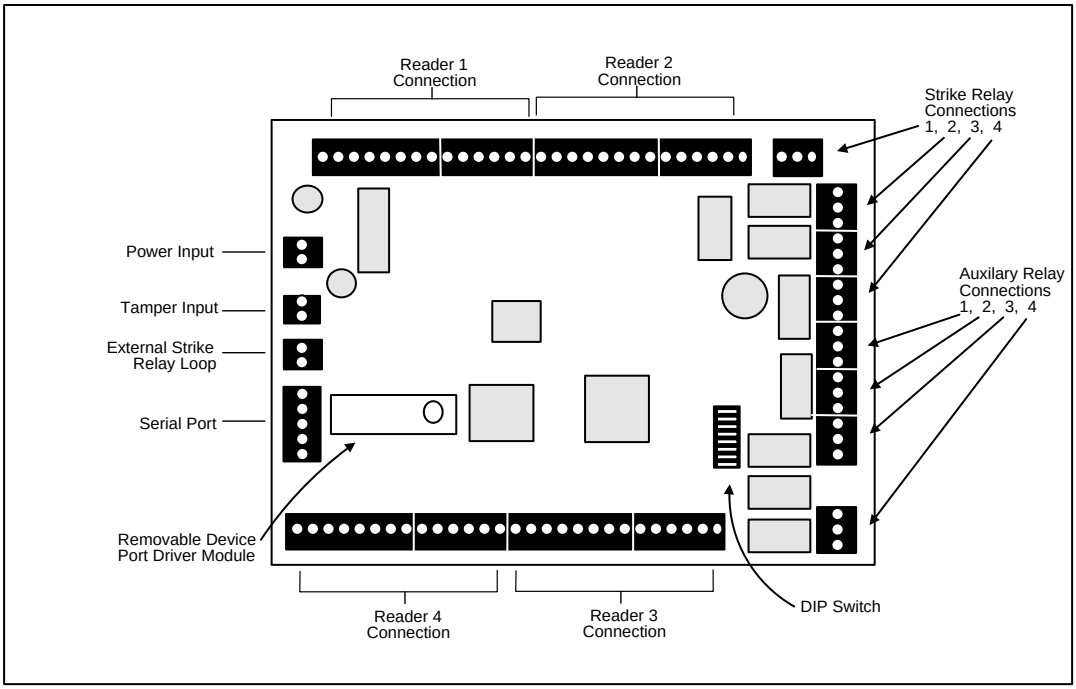


Figure 2.1 AAN-4 Diagram. Terminal Connectors, DIP Switch, Output Relays, device port driver connection, and other component locations are shown. In the network configuration (AAN-4N) the removable port driver module is replaced with an ENI-100 Network Interface module.

2.1 Terminal Connectors

The AAN-4 has 9 terminal blocks for connecting power, reader and alarm inputs, and relay output connections. The connection terminals are factory equipped with removable screw-down quick connectors which are easily removed from the board by firmly grasping the connector and pulling away from the board. If pliers are used to remove the connectors, they should be of the rubber-tipped type. Take care in using any tools near the board not to damage on-board components. The proper location of the quick connectors is outlined in white on the board.

AAN-4 Terminal Connections			
Reader Connections			
Position	Type	Label	Function
1	Ground (Reader Power)	GND	Reader 1 Device Connections
2	Green LED Control	GLED	
3	Beeper (Buzzer) Control	BZR	
4	Wiegand Data 1	D1	
5	Wiegand Data 0	D0	
6	VDC (Reader Power)	VDC	
7	Red LED Control	RLED	
8	Yellow LED Control	YLED	
9	Auxiliary Input Return	AUXR	Reader 1 Auxiliary Input (Normally Closed)
10	Auxiliary Input	AUX	
11	Exit Push Button Return	EPBR	Reader 1 Exit Push Button (Normally Open)
12	Exit Push Button	EPB	
13	Door Contact Return	DCR	Reader 1 Door Contact (Normally Closed)
14	Door Contact	DC	
15	Ground (Reader Power)	GND	Reader 2 Device Connections
16	Green LED Control	GLED	
17	Beeper (Buzzer) Control	BZR	
18	Wiegand Data 1	D1	
19	Wiegand Data 0	D0	
20	VDC (Reader Power)	VDC	
21	Red LED Control	RLED	
22	Yellow LED Control	YLED	
23	Auxiliary Input Return	AUXR	Reader 2 Auxiliary Input (Normally Closed)
24	Auxiliary Input	AUX	
25	Exit Push Button Return	EPBR	Reader 2 Exit Push Button (Normally Open)
26	Exit Push Button	EPB	
27	Door Contact Return	DCR	Reader 2 Door Contact (Normally Closed)
28	Door Contact	DC	

AAN-4 Terminal Connections			
29	Ground (Reader Power)	GND	Reader 3 Device Connections
30	Green LED Control	GLED	
31	Beeper (Buzzer) Control	BZR	
32	Wiegand Data 1	D1	
33	Wiegand Data 0	D0	
34	VDC (Reader Power)	VDC	
35	Red LED Control	RLED	
36	Yellow LED Control	YLED	
37	Auxiliary Input Return	AUXR	Reader 3 Auxiliary Input (Normally Closed)
38	Auxiliary Input	AUX	
39	Exit Push Button Return	EPBR	Reader 3 Exit Push Button (Normally Open)
40	Exit Push Button	EPB	
41	Door Contact Return	DCR	Reader 3 Door Contact (Normally Closed)
42	Door Contact	DC	
43	Ground (Reader Power)	GND	Reader 4 Device Connections
44	Green LED Control	GLED	
45	Beeper (Buzzer) Control	BZR	
46	Wiegand Data 1	D1	
47	Wiegand Data 0	D0	
48	VDC (Reader Power)	VDC	
49	Red LED Control	RLED	
50	Yellow LED Control	YLED	
51	Auxiliary Input Return	AUXR	Reader 4 Auxiliary Input (Normally Closed)
52	Auxiliary Input	AUX	
53	Exit Push Button Return	EPBR	Reader 4 Exit Push Button (Normally Open)
54	Exit Push Button	EPB	
55	Door Contact Return	DCR	Reader 4 Door Contact (Normally Closed)
56	Door Contact	DC	
Relay Output Connections			
57	Common	C	Door 1 Strike Relay Connection
58	Normally Open	NO	
59	Normally Closed	NC	

AAN-4 Terminal Connections			
60	Common	C	Door 2 Strike Relay Connection
61	Normally Open	NO	
62	Normally Closed	NC	
63	Common	C	Door 3 Strike Relay Connection
64	Normally Open	NO	
65	Normally Closed	NC	
66	Common	C	Door 4 Strike Relay Connection
67	Normally Open	NO	
68	Normally Closed	NC	
69	Common	C	Door 1 Auxiliary Relay Connection
70	Normally Open	NO	
71	Normally Closed	NC	
72	Common	C	Door 2 Auxiliary Relay Connection
73	Normally Open	NO	
74	Normally Closed	NC	
75	Common	C	Door 3 Auxiliary Relay Connection
76	Normally Open	NO	
77	Normally Closed	NC	
78	Common	C	Door 4 Auxiliary Relay Connection
79	Normally Open	NO	
80	Normally Closed	NC	
AAN-4 Device Connections			
81	Power Input	VIN	Power Input Connection
82	Ground	GND	
83	Tamper Input	TMP	Cabinet Tamper Input (Normally Closed)
84	Tamper Input Return	GND	
85	20 mA loop Signal Out	STRK	ADA-10/11 External Relay Loop
86	20 mA loop Signal Return	RET	
87	Receive Data (+)	R+	Host Communication Connection (Serial Mode)
88	Receive Data (-)	R-	
89	Transmit Data (+)	T+	
90	Transmit Data (-)	T-	
91	Signal Ground	SG	

Table 2.1: AAN-4 Terminal Connections.

2.2 DIP Switches

The AAN-4 has one block of DIP switches, with 8 switches. These switches are used to set various configuration options for the interface. It is recommended to power the board down before making any changes in the DIP switch settings as any changes will not take effect unless the power is cycled.

2.2.1 DIP Switch Tables

Communications Address (SW1)					
5	**4**	**3**	**2**	**1**	
OFF	OFF	OFF	OFF	OFF	0
OFF	OFF	OFF	OFF	ON	1
OFF	OFF	OFF	ON	OFF	2
OFF	OFF	OFF	ON	ON	3
OFF	OFF	ON	OFF	OFF	4
OFF	OFF	ON	OFF	ON	5
OFF	OFF	ON	ON	OFF	6
OFF	OFF	ON	ON	ON	7
OFF	ON	OFF	OFF	OFF	8
OFF	ON	OFF	OFF	ON	9
OFF	ON	OFF	ON	OFF	10
OFF	ON	OFF	ON	ON	11
OFF	ON	ON	OFF	OFF	12
OFF	ON	ON	OFF	ON	13
OFF	ON	ON	ON	OFF	14
OFF	ON	ON	ON	ON	15
ON	OFF	OFF	OFF	OFF	16
ON	OFF	OFF	OFF	ON	17
ON	OFF	OFF	ON	OFF	18
ON	OFF	OFF	ON	ON	19
ON	OFF	ON	OFF	OFF	20
ON	OFF	ON	OFF	ON	21
ON	OFF	ON	ON	OFF	22
ON	OFF	ON	ON	ON	23
ON	ON	OFF	OFF	OFF	24
ON	ON	OFF	OFF	ON	25
ON	ON	OFF	ON	OFF	26
ON	ON	OFF	ON	ON	27
ON	ON	ON	OFF	OFF	28
ON	ON	ON	OFF	ON	29
ON	ON	ON	ON	OFF	30
ON	ON	ON	ON	ON	31

Baud Rate		
	7	**6**
1200	OFF	OFF
2400	OFF	ON
4800	ON	OFF
9600	ON	ON

Input Monitor Mode	
	8
Unsupervised	OFF
Supervised	ON

Table 2. 2: AAN-4 DIP Switch Settings

2.2.2 DIP Switch Function

Communications Address—This option sets the address that identifies the device on the communications line. This setting must be specified in the host software in able to identify the device. A **maximum of 16 AAN-4** devices can be installed on one communication line (RS-485), with each having a unique address (between 0-31). The communications address must also be specified in the host software when the AAN-4 is connected though a network. **NOTE: AAN-4 controllers can NOT be used on the same serial communications line as an AAN-100 or AAN-32 controller.**
Baud Rate—Specifies the baud rate for the serial line of interface. This setting must be the same for all devices on the communication line connected to this port.
Input Monitor Mode—Specifies whether all inputs on the interface (Auxiliary inputs, door contacts, exit push buttons) will be monitored by comparing the resistance value of the input line with the expected value. ON—In the event of tampering with the input, the interface will report the specific type of error. OFF—Inputs will operate in standard mode.

Table 2.2.1 : DIP Switch Function

2.3 Connectors

The AAN-4 has several connectors for interfacing with removable components. Take care when installing and removing components in order not to damage pins or sockets. Do not use force greater than gentle pressure when installing any components. Refer to the figure for the exact location of these connectors. The connectors are also labeled on the AAN-4 in white lettering on the circuit board.

2.3.1 Device Port Communication Driver Socket

Port Communication Driver Socket: J12

For communication on the AAN-4, a communication module must be connected to the 12-pin socket. The required module depends on the type of host connection:

Network Communication (AAN-4N) - In order to use network (TCP/IP) connection to the software host, the AAN-4 should be equipped with an ENI-100 Network Interface device. This allows connection to the network via the ENI's RJ-45 jack and a standard UTP Ethernet cable (the RS-485 Host Communication Connection terminals are not used in this mode). In this case, the software host will need two pieces of information to communicate with the hardware: the IP address of the ENI-100 Network Interface (Set by the ENI-100's internal webpage configuration) and the Communication Address (set by DIP switches). The software will first search for the IP address and then will use the Communication Address to find the specified device at that address. In this case there is only one device connected, but it is nonetheless important that the Communication Address is the same in the software as is set on the DIP switches.

Serial Communication (AAN-4S) - To use the AAN-4 in serial communication mode, a serial driver must be connected to the driver socket. The communication driver module can be either ASM-48 (RS-485, part number 430-131) or ASM-23 (RS-232, part number 430-132) depending on the type of communication required on the port. The device is connected to the serial communications line using the Host Communication Connection (see Table 2.1). If RS-232 is used, one device may be connected to the line. If RS-485 is used, a **maximum of 16 AAN-4s** can be connected on one communications line (each having a unique address from 0 to 31). **NOTE: AAN-4 controllers can NOT be used on the same serial communications line as an AAN-100 or AAN-32 controller.**

Module Installation - The desired module should be installed so the long end extends towards the middle of the board and the mounting holes provided on the AAN-4 and ASM or ENI align so a plastic stand-off and screws can be attached to connect the holes. METAL SCREWS AND STANDOFFS SHOULD NOT BE USED TO MOUNT THE ASM/ENI.

2.3.2 Additional Connectors

Additional Connectors/Jumpers: J13, J14

These connectors and jumpers are used for factory configuration and should not be modified or connected in any way unless directed by your technical support.

2.4 LEDs

The AAN-4 has 2 LEDs for use in monitoring functioning of panel and for diagnosis of problems. The LEDs function in two modes: startup and normal operation

2.4.1 Start Up Mode

Immediately after powering on the panel, the start-up test will initiate and the results will be displayed on the LEDs. If there are no failures, the test will progress. If the panel encounters an error, it will stop with the failed test and display the LED sequence corresponding to that test. The test sequence and the LED codes are:

Test	D14	D15
ROM/Firmware	ON	OFF
RAM	OFF	ON
Test OK—Loading Config	ON	ON

Table 2. 4: AAN-4 Start up LED Function

2.4.2 Normal Operation

After initialization and self tests, the LEDs will switch to normal operation and will display information about the panel operation.

Heartbeat (D14)—Shows a constant ‘heartbeat’ (0.2 sec ON, 0.8 sec OFF) to indicate proper operation of the panel and firmware.

Port Status (D15)—Shows activity on the serial port. Normal activity on the ports will be observed as the LED blinks many times a second or lighted solid, depending on the amount of activity.

2.5 Firmware

The operating program for the AAN-4 is stored in re-programmable flash memory. In the event that the firmware must be re-installed or updated, no chips need to be replaced on the panel. The new program can be loaded from the host via special software. For normal operation it is not necessary to update the firmware. If this becomes necessary, contact your Apollo support representative. Firmware updating should only be done under the recommendation and guidance of your Apollo technical support representative.

2.6 Memory Backup

The AAN-4 is equipped with on-board memory to store configuration information and event data. This memory, as well as the real-time clock, is provided with back-up power (for up to 5 days) in the event of primary power failure. Power is supplied by a special capacitor-based circuit. Battery replacement is never required.

2.7 Additional Installation Information

2.7.1 Mounting Holes

Four holes are provided for mounting the AAN-4. Standoffs should be used when mounting in order to protect the underside of the circuit board.

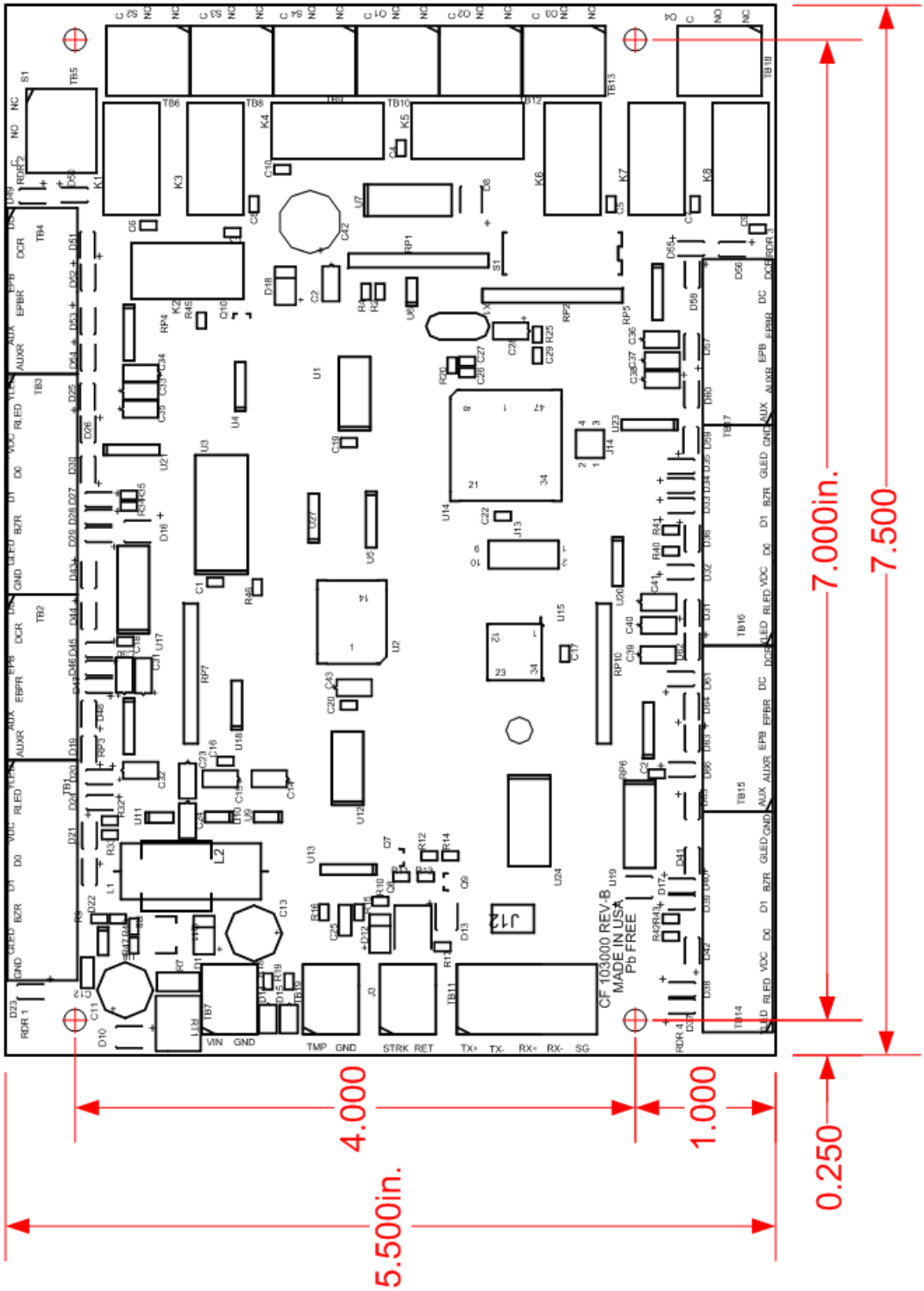
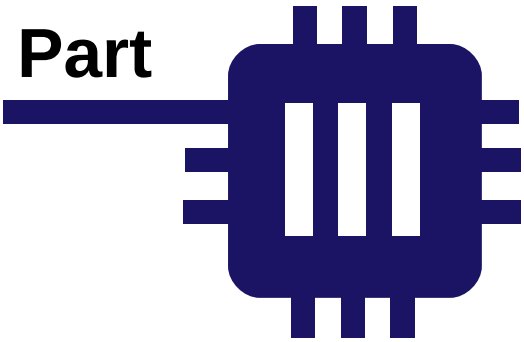


Figure 2.7.1 AAN-4 Mounting Holes. Location of mounting holes for the AAN-4 is shown in scale. *Note that the drawing will not print the exact size of the actual circuit board.*



System Wiring

APOLLO
intelligent security solutions

3 System Wiring

SPECIAL NOTE: To guard personal safety and avoid damaging equipment it is important to have a full understanding of electrical wiring practices and safety. The following sections provide general guidelines relating to the AAN-4, but are not a substitute for complete training in dealing with electrical systems!

3.1 Power

Power Connection: TB7

Power is supplied to the AAN-4 by the voltage connection in terminal block 7 (see Part 2.1 for exact locations of terminals). The power connection should be 12-24 VDC. Power consumption is 250 mA. The AAN-4 is protected from over-current and over-voltage by on-board circuitry.

Take care when selecting a power supply for use with the AAN-4. Most power supplies in the market today provide good input/output isolation, however those which do not provide isolation (or have high leakage capacitance), coupled with accidental AC power lines interchange, present serious ground fault problems for installers. With ground fault, the signal reference between subsystems may be 115 VAc (230 VAc) apart. If these subsystems are interconnected, the large potential difference will cause equipment damage or personal injury. Apollo recommends the use of isolated continuous power supplies only. All Apollo supplied power supply assemblies are transformer isolated for safety and to minimize ground loop problems.

In the case of over-current, solid-state fuses integrated on the AAN-4 panel will ‘trip’ to protect the components of the panel. In many cases, the solid-state fuses will reset automatically when normal current resumes, however it may be necessary to interrupt the supply of power to allow the fuses to reset.

3.2 Grounding

Special care should be taken when grounding the AAN-4 controller and other devices connected to it via the direct communication lines. Each device must be grounded to provide ESD protection, personnel safety, and signal reference for devices which communicate with each other. Grounding the reader provides a good shield against external transients. There are three types of circuit grounds in systems using Apollo products: DC ground, RS-485 signal ground, and Safety (Earth) ground.

3.2.1 DC Ground

This is typically the minus (-) side of the DC output of the power supply. It is to be connected to the DC ground input of all devices being powered by one supply. It must not be connected in any way to any of the 5 RS-485 signals or the AC side of the line including Safety (Earth) ground (one connection to Safety (Earth) ground is acceptable, but this connection is usually internal in the host computer and should not be introduced externally if direct connection is used (RS-232/485)).

3.2.2 RS-485 Signal Ground (SG)

This is the 5th wire used for the RS-485 communications. It is used to provide a common reference between all devices on the line and should only be connected to each of the devices' SG input. The SG wire must not be allowed to touch any other potential, especially earth ground. The shield drain wire of the RS-485 communications cable is commonly used to connect the SG leads together. Usually this wire does not have an electrical insulator. It is important that the SG wire is thoroughly insulated by the installer at all connection points. Improper insulation of this conductor may allow accidental shorting to earth ground through conduit or other metallic components, causing intermittent communications or equipment damage.

3.2.3 Safety (Earth) Ground

Safety ground is part of the AC power system. To avoid ground loop current, there must be only ONE point at which the safety ground connects to the DC ground.

The RS-485 signal ground must be isolated from the safety ground. This means that the RS-485 cable shield drain wire must be insulated at connection points so that it will NOT accidentally short circuit to the conduit in instances where the conduit is connected to the safety ground. (See Figure 117)

Please check the applicable regulations and legislation in your country prior to installing the AAN-4 controller and other Apollo products. In the US, the National Electrical Code, as well as other safety regulations, require that all equipment chassis and/or enclosures be grounded in order to prevent electrical shock hazards. Each device must have a green wire safety ground. The function of the green wire safety ground is to provide a redundant path for fault currents and to insure that the circuit breaker will open in the event of a fault. In addition, grounding the enclosure provides a path for ESD dissipation, thus protecting sensitive electronic devices. (See Figures 115 and 116)

3.2.4 Grounding System

A grounding system can be viewed as two subsystems: the DC system and the Ground System. The DC system consists of all interconnected power supply returns, DC distribution wiring, and load devices. The principal function of the DC system is to provide signal reference for communication. The Ground System consists of all chassis grounds for power supplies and other devices, safety grounds, and AC grounds. Ground connection should be made to avoid ground loop problems. (See Figure 115)

Ideally, there should be ONLY ONE ground return point in a power supply system. In a system with a PC (personal computer), it is likely that the PC already provides the DC Ground connection to the Ground System (earth ground). Care must be taken NOT to create more ground connections. In systems with multiple PCs communicating to Apollo Hardware via direct connection, the ground potential must be the same for inter-connection, or some form of isolation must be provided.

3.2.5 Grounding Potential Difference Checks Before Connecting

Before a device is connected to an RS-485 subsystem, it must be checked for ground fault. Uncorrected ground fault can damage all devices connected to the RS-485 communication line.

To check if there is ground fault for a new unit, follow the steps below (See Figures 105, 113, 115, 116 and 120):

1. Apply power to all devices already successfully connected to the RS-485 line.

2. Power up the new unit, but DO NOT connect it to the RS-485 line.

3. Connect the signal ground (SG) of the RS-485 line through a 10k limiting resistor.

4. Measure the AC and DC voltage across the resistor. There should NOT be more than 1 volt across the resistor. Otherwise find and clear the fault.

5. Connect the new unit to the RS-485 line only if no ground fault is found.

3.3 Host Communication Connection

The connection from the AAN-4 to the programming host (PC) is used for programming the panel and then monitoring the status of the system. Once a connection is established, the host software communicates with the panel and transmits the necessary configuration information. Once this is established, the host and panel will maintain a constant communication until it is terminated by the host. While connected, the controller will send events in real-time after a request from the host. The controller will not send information to the host unless a request is received. These events will be ‘buffered’ in the memory of the controller until the host is ready to receive. Thus, all system events are protected and will not be sent to a host that is not ‘listening’, therefore losing events.

The connection can be made either by serial connection (using the Host Communication Connection) or by Ethernet (using the RJ-45 jack of the ENI-100 Network Interface Module).

3.3.1 Serial

Using the Host Communication Connection (and an ASM-32 or ASM-48 driver), the connection from the AAN-4 to the host can be made using RS-232 or RS-485 protocols. The choice to use RS-232 or RS-485 depends on many factors for the particular installation. The main differences are outlined below:

	RS-232	RS-485
Maximum Distance	50 Feet (15 Meters)	4000 Feet (1200 Meters)
Devices Per Line	1	16 (AAN-4S is limited to maximum 16 devices on one serial line)
Communications Port	Standard on Many PCs	Requires Adapter (RS-232 to RS-485) or Add-on PC Card
Data Rate	20K Bps	10M Bps

After choosing the method of communication, the proper wiring must be made from the host to the controller. Typically, the communication will be from a standard 16550 UART COM-port on a PC which will be connected directly to the AAN-4 in the case of RS-232 or through the use of an adapter or add-on PC card to achieve the RS-485 signal. The communications wiring must cross-over from the PC to the panel as shown in Figure 3.3.1.

The connection originating from the host PC will then be connected to the Host Communication Connection (see table 2.1). Ensure that the proper communications driver is installed in J10 (ASM-48, part number 430-132, for RS-485, ASM-23, part number 430-131, for RS-232). When communication established, the activity will be seen on the comm activity LED. The blinking rate of the LED will vary at first as communication is established and configuration is updated, and then should blink at a steady rate of several times per second.

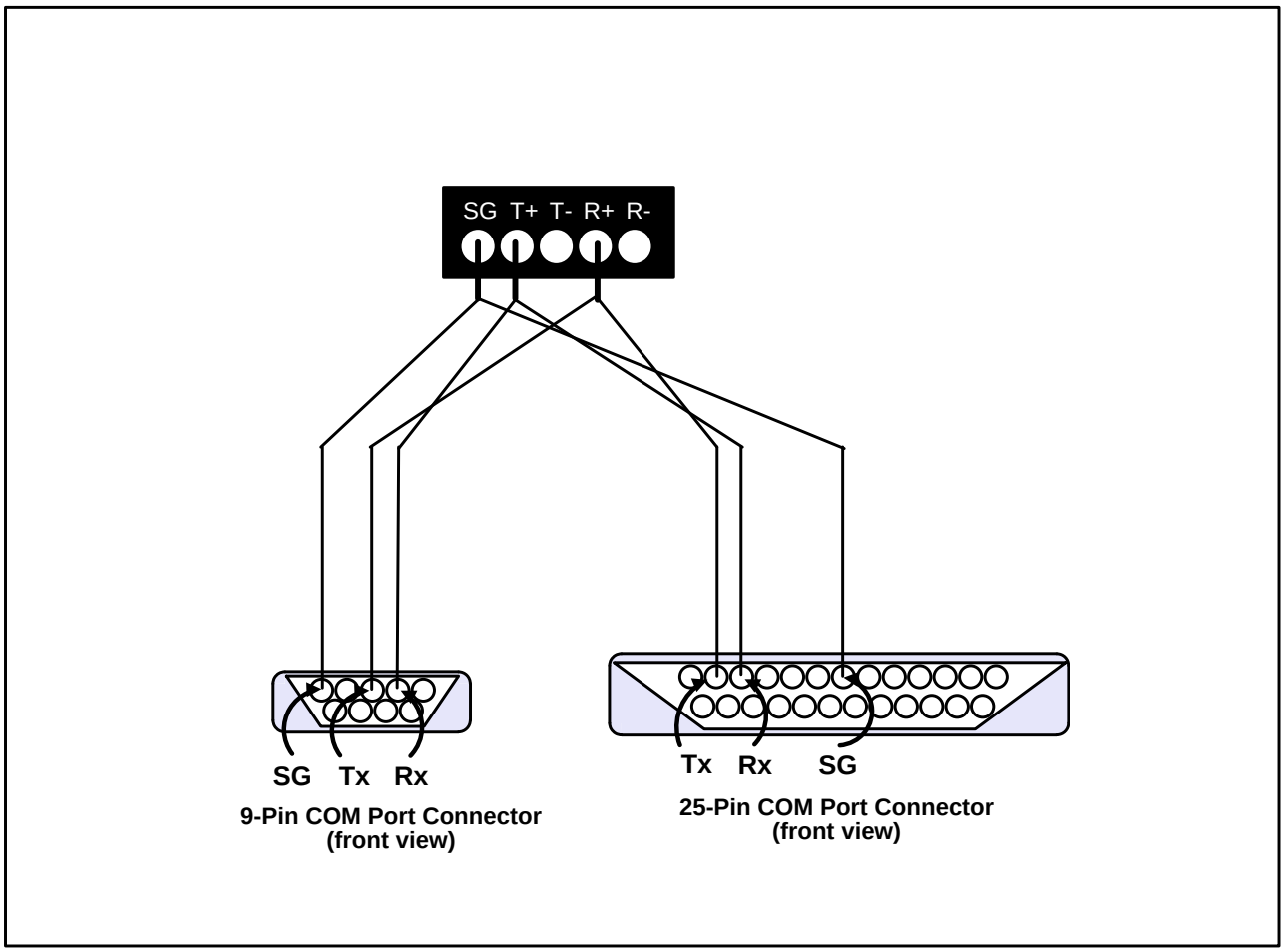


Figure 3.3.1 Host to AAN-4 Serial Wiring Pinouts (RS-232). The wiring from the host to the panel must be done according the type of host port (RS-232 or RS-485, 9-pin or 25-pin) and then properly connected to the Host Communication Connection. Refer to the Terminal Connector table for position of the required RS-485 connections.

3.3.2 Network

For connection from the host to the AAN-4, an ENI-100 Network Interface Module is used. The ENI-100 acts as a standard Ethernet network device and occupies one IP address (see Part 4 for programming instructions). The connection from the ENI to the network is made by a standard RJ-45 jack. A standard UTP network cable should be connected from the ENI-100 to the local network via a network switch, hub or other network connection device. The ENI communicates at 10/100Mbps with the TCP/IP protocol. The IP address of the ENI should be specified in the host software and the host will initiate communications with the ENI, which will translate the messages to the AAN-4.

Routing with ENI-100: If the ENI has an IP address that is not on the same subnet as the host computer, there is no need to program a gateway in the ENI as it does not originate communication in this configuration. If the proper network path is established from the host to the ENI, (including necessary gateways) the ENI will receive the communication from the last router or gateway in the path. This router or gateway will deliver the message to the ENI with the IP address of the host computer, but with the router or gateway's own MAC address. The ENI will reply to the IP of the host computer, but directed to the MAC address of where the message originated (the router or gateway). The reply will then be sent by the router or gateway on the correct path back to the host.

3.3.2.1 ENI-100

3.3.2.1.1 Introduction

The ENI-100 Network Interface Module provides connectivity between the AAN-4 and programming host via TCP/IP interface at 100Mbps. The ENI-100 converts the output signal from the AAN-4 to TCP/IP packets and converts incoming packets, received from the host, into the proper signal.

3.3.2.1.2 Hardware Layout

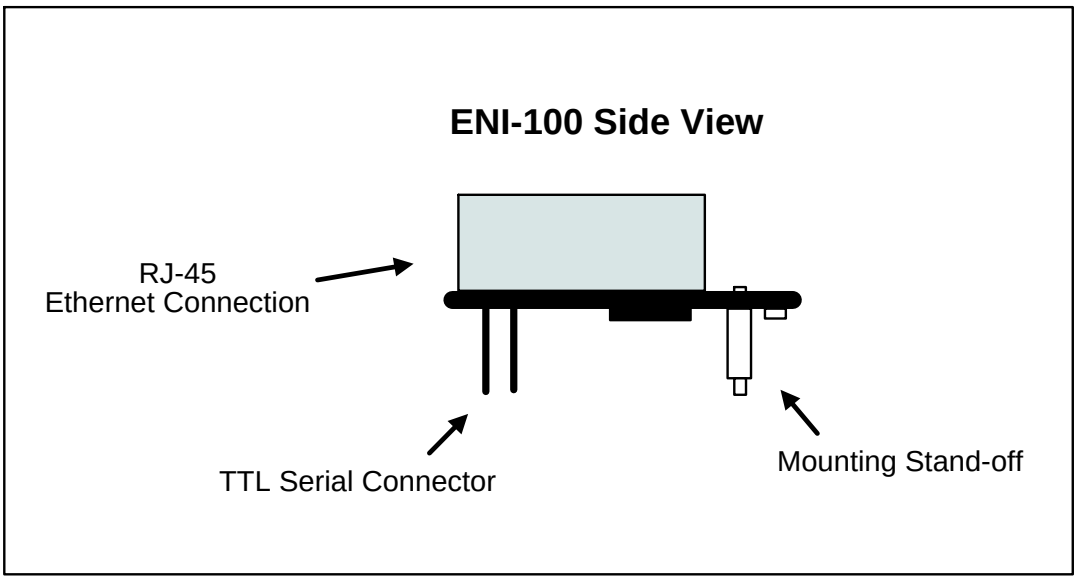


Figure 3.3.2 .1: ENI-100 Hardware Layout

3.3.2.1.2.1 Connectors

TTL Serial Connector

12-pin connector located on the underside of the ENI used for connection to port J12 on the AAN-4N. Communication AND power are supplied through this connector.

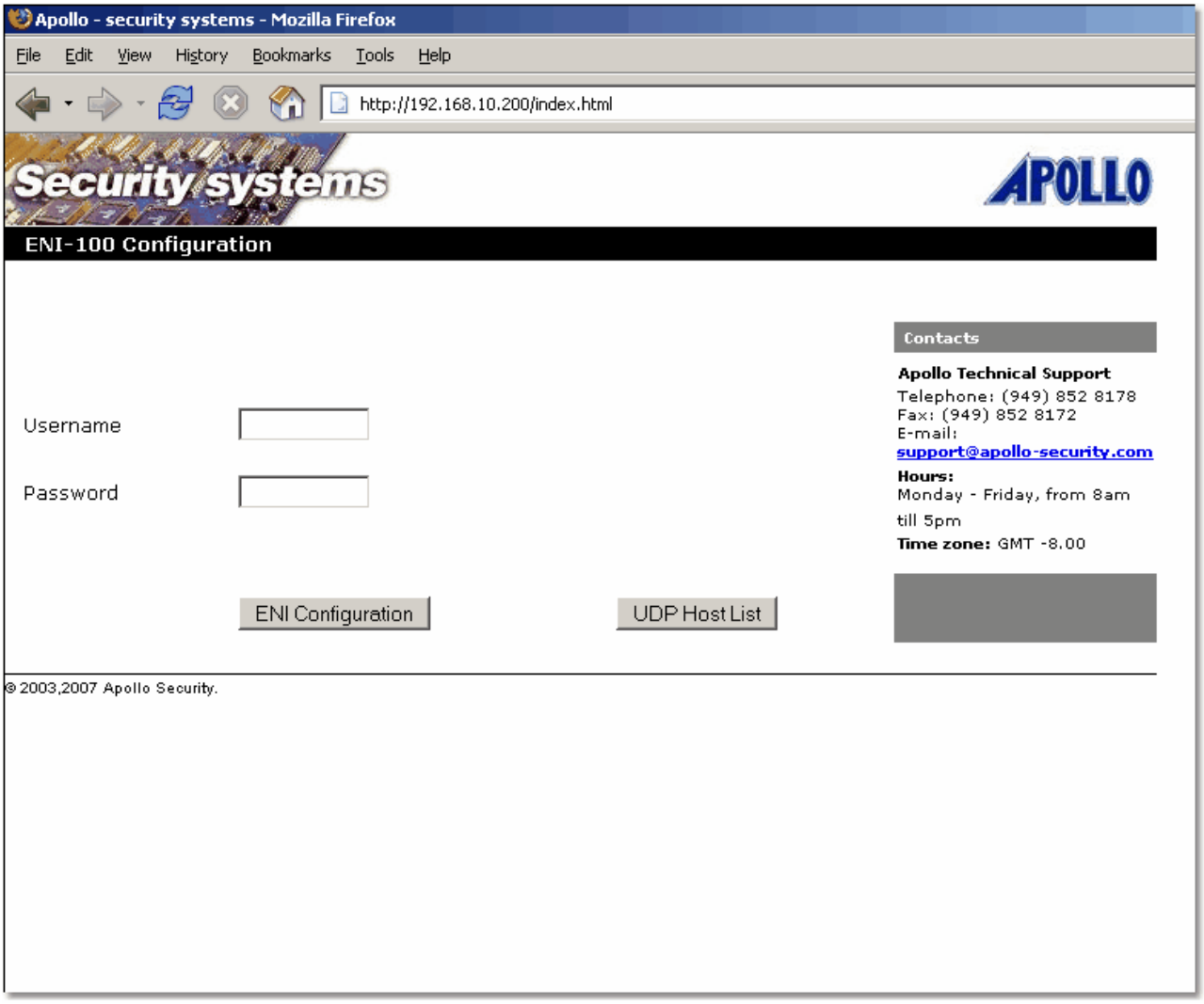
RJ-485 Jack

For communication to the network backbone a standard RJ-45 female connector is provided. The ENI-100/110 communicates at 10 or 100Mbs over standard Ethernet networks.

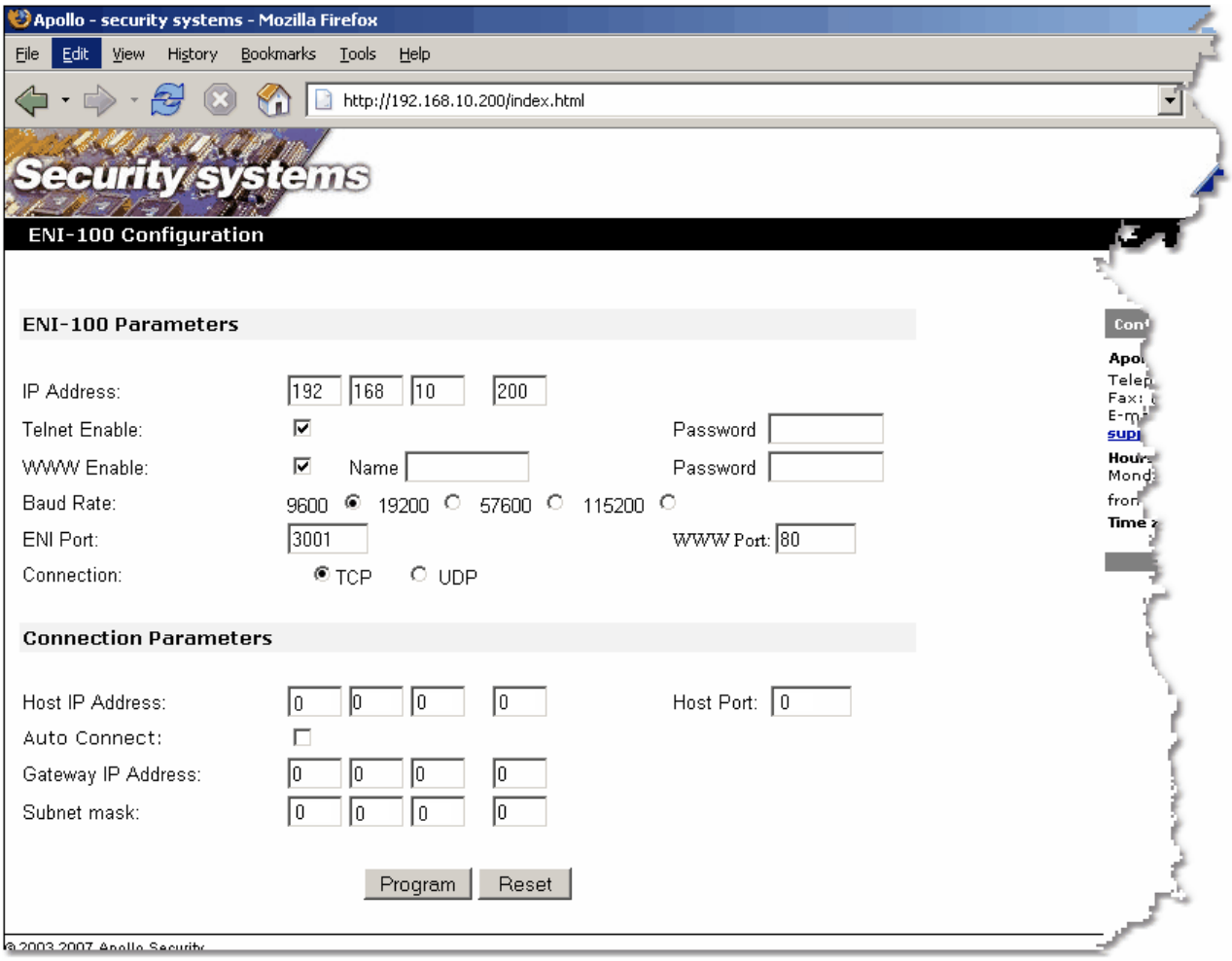
3.3.2.1.3 Communication Configuration

Once the ENI-100 IP address is setup (see the *Software Configuration Utilities* section), communication configuration can be done with a web browser via the ENI's internal web server. For setting additional security parameters, see the *Telnet* section of *Software Configuration Utilities.*

To open the web page configuration, type the IP address of the ENI in the address bar of your web browser. Do not preface the address with “www”. You should see the following screen where the username and password must be entered. The default username/password is blank, thus if it was not previously modified, simply click on “ENI Configuration”.



The ENI main configuration page specifies the mode of operation for the ENI. When all settings have be set as desired, click the "Program" button to save the settings. Clicking "Reset" will change all parameters on the page to their previous values.



ENI-100 Parameters:

> **AAN-4 Standard Settings -** The ***italicized settings*** below will need to be set for standard configuration for use with the AAN-4. Other settings may be necessary or desired, according to your configuration:

IP Address: IP address of the ENI-100. This is a static IP address so the network administrator must verify that it will not be used elsewhere in the system.

Telnet Enable: When checked, enables Telnet access to the web page and configuration files stored in the ENI.

Telnet Password: Password that must be entered to log in the Telnet server in the ENI. *NOTE: No user name is used for Telnet access.*

WWW Enable: When checked, enables web page access for configuring the ENI.

WWW Username and Password: User name and password that must be entered to access the

configuration via the web page.

Baud Rate: The baud rate that the ENI will use to communicate on the serial port. This setting must match the baud rate of the programming host. ***Required: 9600***

ENI Port: The TCP port number that must be used to open a network connection to the ENI. This should be an unused port on your network. Consult your system administrator for more information. ***Recommended: 3001 - must match setting in software***

WWW Port: The HTTP port that the web server will use to display the configuration pages. The default value is 80 which is used by default by most web browsers. If it is necessary to set another port, it will be necessary to specify the port when accessing the configuration page. For example, if port 8080 were used, it would be necessary to specify this port in addition to the IP address such as entering in the browser address bar: http://192.168.10.177:8080.

Connection: Select either a TCP or UDP connection. TCP communication is used for AAN-4 to host communication. ***Required: TCP***

Connection Parameters

Host IP Address/Port: *When auto-connect is enabled*, this is the first host address of another ENI device which a connection will be established with. Set all values to '0' to disable this feature. *When Auto-connect is not enabled*, this is used to limit which hosts may connect to the ENI. All zeroes means that any host may connect. ***With the AAN-4, auto-connect should be disabled thus only the host limiting function can be used.***

(The following settings should not be used with the AAN-4)

Auto Connect: If checked will cause the ENI to automatically connect to the Host Address given. This address should be another ENI that is *not* set to auto connect. ***Required: Not enabled.***

Gateway Address and Subnet Mask: These are used to connect to another ENI that is not on the same network when the Auto Connect box is checked. Set all values to '0' to disable this feature. ***Required: Not enabled.***

UDP HOST LIST

From the main screen clicking the “UDP Host List Button” will display the Host List configuration. This feature is not used by the ENI-100 when used with the AAN-4.

After changing any of the above configuration options, click the “program” button at the bottom of the page. The ENI will then save the settings and will be reset. Clicking the “Reset” button at the bottom of the page will reset the values to their current configuration. If you do not wish to change any configuration options, simply close the browser window without pressing either button.

3.4 Card Reader Wiring

Up to four card readers can be connected to the AAN-4. Card readers with standard Wiegand output are supported, including magnetic stripe, proximity, bar code, smart card, biometric, keypad, etc. It is not necessary for the readers to be identical on each connection port, i.e. up to four different reader types can be used simultaneously.

Each reader connection consists of connection terminals for VDC Output and Ground, Data 1 Signal, Data 0 Signal, Beeper control, and multiple LED control (red, green, and yellow). The wiring to the reader should be made using 24 AWG shielded cable with 4 twisted pairs (Belden 9504 or equivalent). Do not exceed 500 feet (152 m) between the AAN-4 and reader. Connect the shield drain wire of the cable at the GND terminal of the appropriate reader connector on the AAN-4. Carefully insulate the drain wire with sleeving for a reliable

installation.

Power for the reader connection (VDC) is derived from the power input (VIN) for the AAN-4 and is distributed between the four reader connections. *Thus, voltage to the reader power connection will roughly equal the voltage supplied to the AAN-4 power input.* There must be sufficient power to supply the load of all readers as well as for the AAN-4 itself (+12 to +24VDC @ 250 mA). If the readers have a greater total power requirement, or if there are other wiring concerns, external power supplies should be used to power the readers. In this case, only connect the reader power lines to the external power supply; do not connect the reader to two power supplies.

For basic operation of the reader, at a minimum the Data 0 and Data 1 wires must be connected from the reader to the AAN-4 and power supplied to the reader. LED and beeper control lines do not have to be connected, but in this case, the LEDs and beeper may not function on the reader.

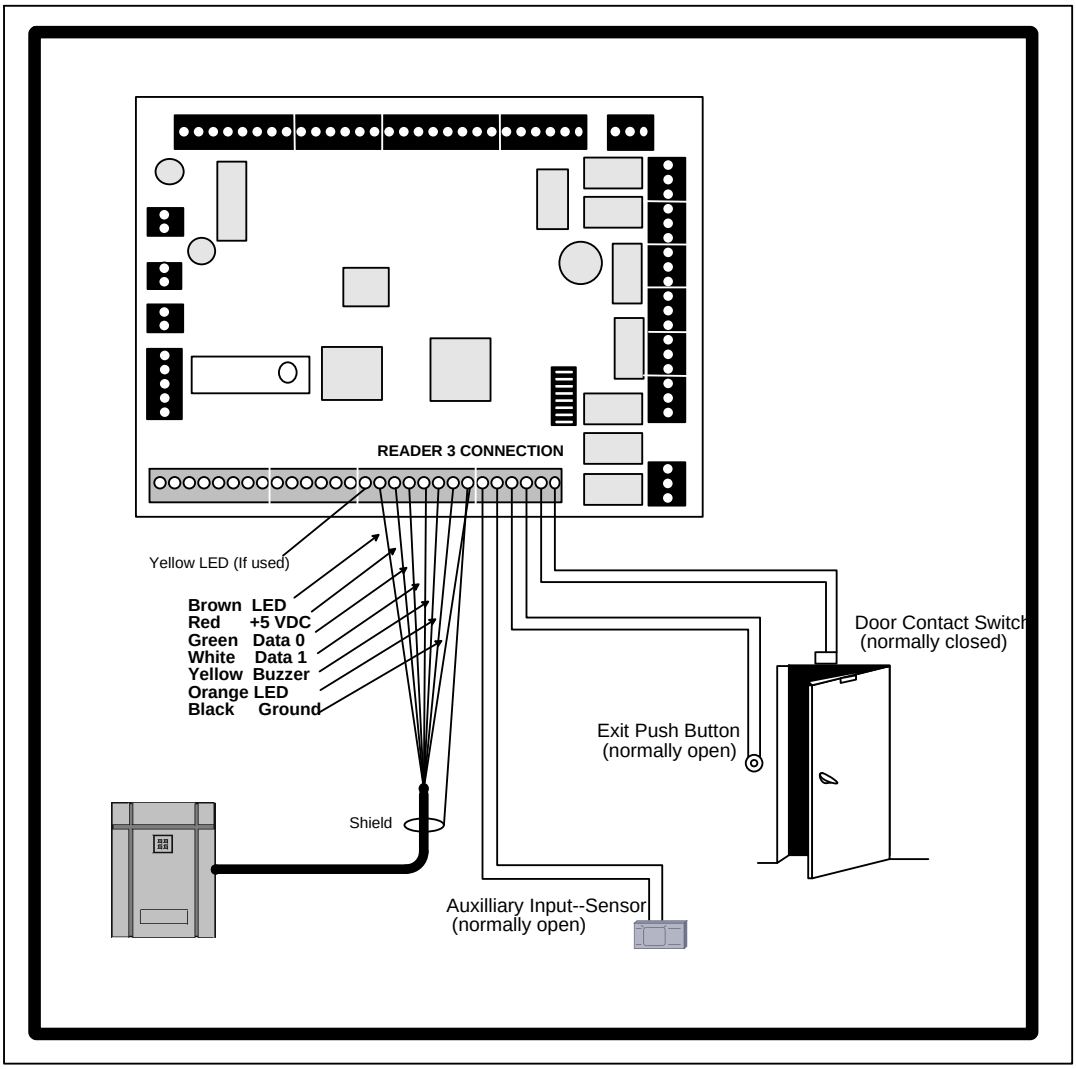


Figure 3.5 AAN-4 Card Reader and Input Wiring. The AAN-4 supports up to four card readers which are connected in standard configuration. For each reader connection there is a door contact input, exit push button input and one axillary input which is displayed here connected to a motion sensor. Refer to the Terminal Connectors table and the installation instructions for the reader that will be used for exact wiring positions.

3.5 Reader Input Wiring

The each of the four reader inputs on the AAN-4 has three input circuits (Door Contact, Exit Push Button and Auxiliary Alarm 1). These inputs can be configured as UL Grade “B” (unsupervised) or UL Grade “A” (supervised). The selection of supervised / unsupervised is made by changing DIP switch number 8. If in the OFF position, the inputs for **all** readers are configured as unsupervised, if in the ON position **all three** inputs are configured as supervised. It is not possible to have both unsupervised and supervised inputs at the same time, all inputs must be in the same configuration. If the inputs are configured as unsupervised, the door contact, exit pushbutton, and both auxiliary alarm contacts should be connected directly to the wiring terminals without using any end of line terminating resistors. If the inputs are configured as supervised, the contacts must be connected to end of line terminating resistors before being connected to the input terminals. Use of ATM-30 (part number 470-031) terminator is recommended.

3.5.1 Input Supervision (Overview)

Unsupervised, normally closed inputs will have a short circuit (0 ohms) when the circuit is in the secure state and an open circuit (infinite ohms) when the circuit is in the unsecured state. This is a simple connection that does not require addition of any resistors. The drawback to this type of connection (unsupervised) is that if the two wires touch together (either accidentally or intentional sabotage) the reader will permanently detect the circuit as being in the secure state. This effectively prevents all alarm generation. This situation is not very secure and should not be used in any situation that requires maximum security. Unsupervised, normally open inputs will have an open circuit (infinite ohms) when the circuit is in the secure state and a short circuit (0 ohms) when the circuit is in the unsecured state. The same situation will occur as stated above if the wires are cut (permanent secure). Very low security.

The AAN-4 reader interface allows configuration of the inputs to the “supervised” mode. This is designed to prevent the security breach that is possible using the “unsupervised” mode mentioned above. In the supervised state, normally closed inputs will have approximately 300 ohms when in the circuit is in the secure state and 10K ohms when in the unsecured state. If the wires are shorted together or cut (accidentally or intentionally) the reader will instantly detect this (0 ohm or infinite ohm) condition and immediately report this as a circuit fault. The reader will not confuse this condition with a valid secure condition. Normally open, supervised inputs should be 10K ohms when secure and 300 ohms when unsecured. Either way, security is greatly enhanced. TO TAKE FULL ADVANTAGE OF THE INCREASED SECURITY PROVIDED BY INPUT SUPERVISION, THE END OF LINE TERMINATING RESISTORS SHOULD BE ON THE EXTREME END OF THE CABLE, FARTHEST FROM THE READER. In many cases it is possible to mount the resistors inside the housing of the input device.

NOTE: ATM-30 end of line resistors (or an equivalent substitute) are designed to work with the AAN-4 supervision values on STANDARD AAN-4 interfaces. The AAN-4 is available by special order with custom resistor values. In the case of improper function of the supervision, verify what type of AAN-4 is installed in the system.

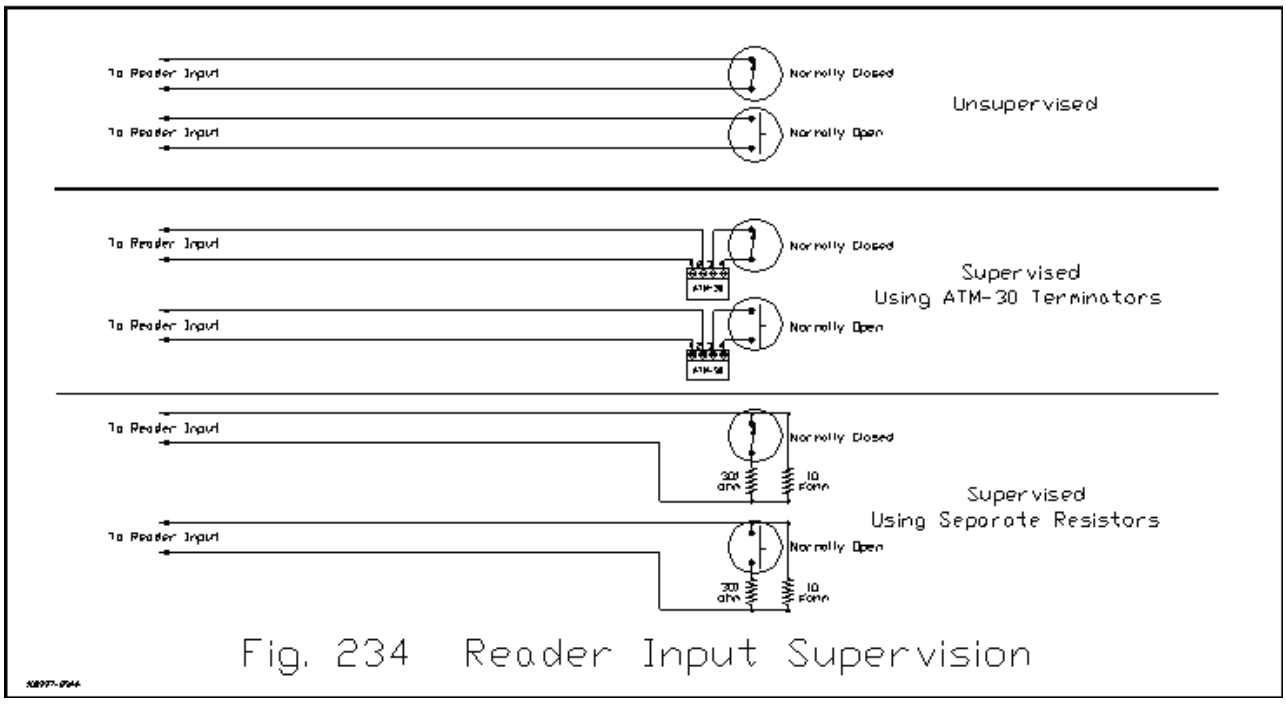


Figure 3.6 Input Supervision. The AAN-4 reader inputs can be configured for Supervised or Unsupervised. End of line resistors must be used in the supervised configuration in order for the circuits to report the correct state.

3.5.2 Door Contact Input (Door Position Switch)

This is a normally closed input and should have a jumper installed if not used!

Terminal connectors: DC, DCR (See Table 2.1)

The door contact input is a normally closed input used to monitor the open/closed status of the door. This will typically be connected to a magnetic sensor in the frame of the door that will provide a short circuit when the door is closed and an open circuit when the door is opened. If input supervision is enabled (see Part 3.6.1 above), end of line terminating resistors must be installed. The terminating resistors should be installed at the door contact end (not the reader end) of the cable.

The reader will use this input to detect when the door is opened and when the door is closed. This information is processed by the reader and used to generate certain alarm messages. If a door is detected to be opened for no apparent reason (not as a result of a valid card or PIN use or exit button activation), the reader will generate a “Forced Open” message. If the door is opened as a result of a valid access request or exit button activation but not allowed to close within the programmed held open time, a “Held Open” alarm will be generated.

The reader may also be configured from the host software to allow early strike relay shutoff. Normally the amount of time that the reader will keep the strike relay activated is controlled by the “Strike Time” setting in the host computer. This is the amount of time a person has to open the door after being granted access. This time is adjustable from 0 to 255 seconds (0 = ½ second). If the strike time is configured for 10 seconds (for example) and the person has already opened and closed the door after 5 seconds, the reader may be configured to terminate the normal 10 second strike time early (thus not allowing the door to be opened twice). If the reader is configured for this early strike shutoff option, it is important that the door contact input is working properly. If the input is not connected or is malfunctioning and the reader detects that the door is always open, erroneous alarms will be generated and the Strike Time will always be very short (the reader thinks the people are opening the door quickly), resulting in it being impossible to open the door.

3.5.3 Exit Pushbutton Input (Request To Exit, REX)

The Exit Push Button input will be disabled during Reader Tamper and for 1 minute after tamper condition ends!

Terminal Connectors: EPB, EPBR (See Table 2.1)

The Exit Pushbutton input is used by the reader to inform the reader of a door opening without first using the card / PIN. Normally, if the reader detects a door open condition without valid use of card or PIN, it will generate a “Forced Open” alarm. This alarm must be masked (inhibited) when people use the door to exit from the inside of any secured area. The Exit Pushbutton input is used for this purpose. After detecting a closed circuit of the Exit Pushbutton input, the reader will ignore the door contact input for a period of time equal to the strike time set for the reader. This allows the people to then open the door for exit without an alarm being generated.

In some situations the Exit Pushbutton input should also close the strike relay to allow the door to be opened from the inside. This feature is configured in the host software. The reader can be programmed to only mask the forced open alarm, or to activate the strike relay and mask the forced open alarm. Use of PIR motion exit devices require that special care be taken in regards to activation of the strike relay. If the reader is configured for activation of strike relay on exit, and a PIR is installed on the interior side of the door for automatic exit activation, if a foreign object is slid under the door from the unsecured side and moved around, the PIR may be activated. This will mask off all door alarms and release the strike relay, allowing unauthorized entry. Use of Fail Secure Strikes (require power to hold door closed) or Magnetic type locks generally will require activation of the strike relay.

Most local fire codes require that exit must be obtainable from all doors regardless of proper operation of the access control system and without any prior knowledge of the system operation. This normally means that some form of emergency crash bar or manual door release be provided. IT IS THE RESPONSIBILITY OF THE INSTALLER TO INSURE ALL LOCAL CODES ARE FOLLOWED DURING INSTALLATION.

3.5.4 Auxiliary Alarm Inputs

This is a normally closed input and should have a jumper installed if not used!

Terminal Connectors: AUX, AUXR (See Table 2.1)

Each reader input on the AAN-4 includes one Auxiliary Alarm circuit. These inputs may be used for many purposes that can be configured in the host software. The capabilities will depend on the particular software system in use. Normally these inputs will be used for monitoring external alarm points such as motion detectors or glass break detectors. They may also be used as input triggers for Internal Variable and Reaction linkage when used with the APACS software. A switch contact may be connected to an Aux Alarm input on reader 4 and the software can be configured to close a relay on reader 23 for example. The full capabilities of the Aux Alarm inputs are described in the software manuals. Specifically, reference the Internal Variable and Reactions portions of the APACS software manuals.

In the default configuration of the AAN-4, this input will be linked to the corresponding Auxiliary Output i.e. Reader 1 Auxiliary Input-Auxiliary Output 1. Thus, if the input is in alarm state (open) the output will be energized. This feature is configurable through the host software so that the auxiliary output can respond to other inputs within the system. For more information consult your software documentation.

3.6 Output Relay Wiring

The AAN-4 has eight output relays onboard, with a dedicated strike relay and an additional Auxiliary Output relay for each of the four readers. In addition to these onboard relays, external high security relay modules can be substituted. The AAN-4 can support a mixture of use of onboard and external relay modules.

3.6.1 Strike Wiring, General

Typically, doors are held closed and released by one of two methods. An electric door strike is installed in the door frame, replacing the mechanical strike plate. This type of strike has a “gate” that is normally held closed and is released by command from the reader. This allows the door to be opened. A second type of lock is a electro-magnetic lock which is a two piece device mounted on the perimeter of the door. A solid plate is mounted to the door and a electro-magnetic lock is mounted adjacent to the plate on the frame of the door. The electro-magnetic lock firmly holds the plate mounted to the door, holding it closed until the power is removed by the reader, allowing the door to be opened.

Most electric locks are available in two configurations, Fail-Safe and Fail-Secure. Fail-Safe locks require power to hold the door closed and will release the door when power is removed. This type of lock will open the door if a power outage occurs. This is desirable for doors used as emergency exits. Fail-Secure locks hold the door closed automatically and require power to release the door. This type of lock is desirable for securing doors in high security applications. Electro-Magnetic locks are typically only available in the Fail-Safe configuration.

Electric locks are also available in a range of operating voltages. 12 volts DC or 24 volts DC are the most common. AC power strikes are also available but are not widely used because of the difficulty in connecting suppression circuitry (see Part 3.6.5.2) and the inability of providing battery backup power in the event of power failure. If a 12 or 24 volt DC lock is selected, the same power supply used to power the lock may be used to power the reader. UNDER NO CIRCUMSTANCES SHOULD AC POWER BE APPLIED TO THE AAN-4 READER INTERFACE!

A typical electric door lock (strike) will require approximately 250 mA. (.250 amps) to control. The relay contacts on all Apollo relays are capable of switching up to 24 volts DC at up to 2 amps. If the particular locking device requires more that 2 amps to control, a separate, external relay capable of switching the required amount of current must be installed.

The AAN-4 provide two methods of strike control for each reader. The first method is by use of the internal strike relay. Four such relays are provided on the AAN-4—one for each reader input. Each is rated for switching 2 amps at up to 24 volts DC. Connection of this internal relay is covered in Part 3.5.3 The reader also has the capability of connecting external, high security relay modules (ADA-10/11) for control of the electric lock as well as other outputs. Connection of these external relays is covered in the following sections. Use of the internal relay provides for a simple, cost effective method for connection of the door strike with a reduced level of security. If someone physically access the strike relay wiring, they may be able to release the door. The external relays (ADA-10/11) are designed to eliminate this possible security breach.

Wiring between the strike power supply, strike relay (internal or external) and the electric lock should be of sufficient gauge to prevent excessive voltage drop under all circumstances.

ALL ELECTRIC LOCKS MUST HAVE A SUPPRESSION CIRCUIT INSTALLED TO PREVENT EXCESSIVE INTERFERENCE WITH OTHER SYSTEM COMPONENTS WHEN THE POWER IS REMOVED. SEE THE FOLLOWING SECTION FOR INFORMATION ON SUPPRESSION INSTALLATION.

3.6.2 Strike Suppression Installation

Most electric locks consist of several components, one of which is usually a coil of wire that acts as an electro-magnet to either release the door (Fail-Secure) or hold the door closed (Fail-Safe). This coil of wire acts as a large inductor. When DC power is applied to a large inductor, energy is stored in the inductor. When the circuit is broken (power is removed) this stored energy is converted to a very large voltage and attempts to travel down the wires connected to the strike. IF SOME METHOD IS NOT UTILIZED TO REDUCE OR SUPPRESS THIS VERY LARGE VOLTAGE, IT CAN CAUSE COMMUNICATIONS PROBLEMS, PERMANENT DAMAGE TO THE STRIKE RELAY, AND PERMANENT DAMAGE TO OTHER SYSTEM COMPONENTS!

The most common method of suppression used on DC power strikes is installation of a reverse biased diode as close a possible to the strike itself. Any type of general purpose diode (1N4001 – 1N4006, etc.) will work

AC powered locks will not allow use of a diode for suppression. There are available suppressors for use with AC powered locks called Metal Oxide Varistors (MOV's). These are sometimes included with the lock. If you wish to use AC powered strikes and a suitable suppressor is not supplied with the lock, you must contact the manufacturer of the lock for information on obtaining a suitable suppressor. Connection of the suppressor should follow the instructions provided with the lock.

3.6.3 Strike Wiring, Internal Relay

The AAN-4 Reader Interface includes internal relays for door strike control for each of the four reader inputs. This relay is capable of switching up to 24 volts at up to 2 amps. If the lock installed on the door requires more than 2 amps to control, an external relay must be provided. The power that is provided to the locking device (strike) through this relay may be connected to the same power supply that is providing power the reader if the strike requires 12 or 24 volts DC. IF THE STRIKE REQUIRES A VOLTAGE OTHER THAN 12 OR 24 VOLTS DC OR ANY AC VOLTAGE, A SEPARATE POWER SUPPLY MUST BE USED.

Use of the internal strike relay allows for simple connection of the door strike without requiring installation of external ADA-10/11 relay modules. This will result in reduced installation costs at the expense of increased security. Use of the external, high-security, relay modules (ADA-10/11) will provide increased security on the strike output.

The diagram below illustrates connection of a DC powered, Fail-Secure, door strike. This type of strike requires power to release the door. The power will be supplied through the normally open (NO) relay contact of the strike relay. No power will be provided to the strike until the reader activates the internal relay. The reader will activate the relay as a result of a valid access request (card swipe, card swipe plus valid PIN, valid PIN entry only, etc.). The reader will also permanently activate the strike relay if commanded by the host software to be "unlocked". The reader may also be configured to activate the relay if the exit pushbutton is depressed. Some software systems may allow configuration of this feature (activate strike relay on exit pushbutton) and others may not.

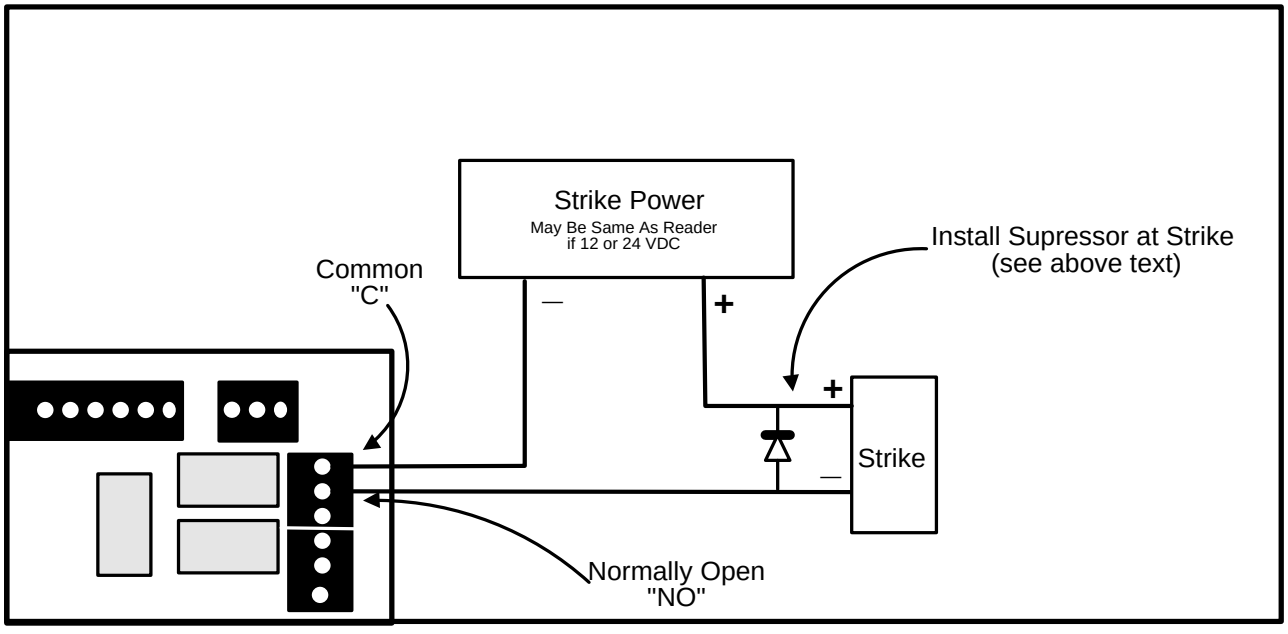


Figure 3.7.3.1 Strike Wiring Diagram - Fail Secure. A wiring example for Fail Secure wiring. Refer to Table 2.1 for exact locations of strike relay connections for the AAN-4.

The diagram below illustrates connection of a DC powered, Fail-Safe, door strike. This type of strike requires power to hold the door closed. The power will be supplied through the normally closed (NC) relay contact of the strike relay. Power will be provided to the strike until the reader activates the internal relay. The reader will activate the relay as a result of a valid access request (card swipe, card swipe plus valid PIN, valid PIN entry only, etc.). The reader will also permanently activate the strike relay if commanded by the host software to be “unlocked”. The reader may also be configured to activate the relay if the exit pushbutton is depressed. Some software systems may allow configuration of this feature (activate strike relay on exit pushbutton) and others may not.

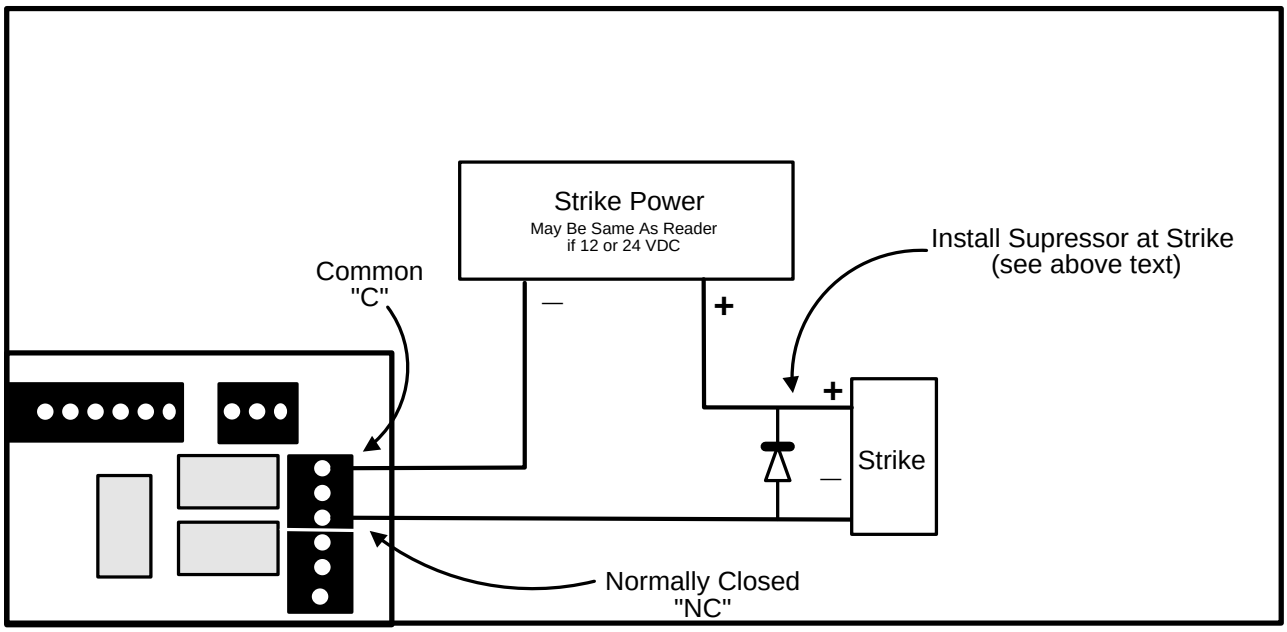


Figure 3.7.3.2 Strike Wiring Diagram - Fail Safe. A wiring example for Fail Safe wiring. Refer to Table 2.1 for exact locations of strike relay connections for the AAN-4.

3.6.4 ADA External High Security Relays

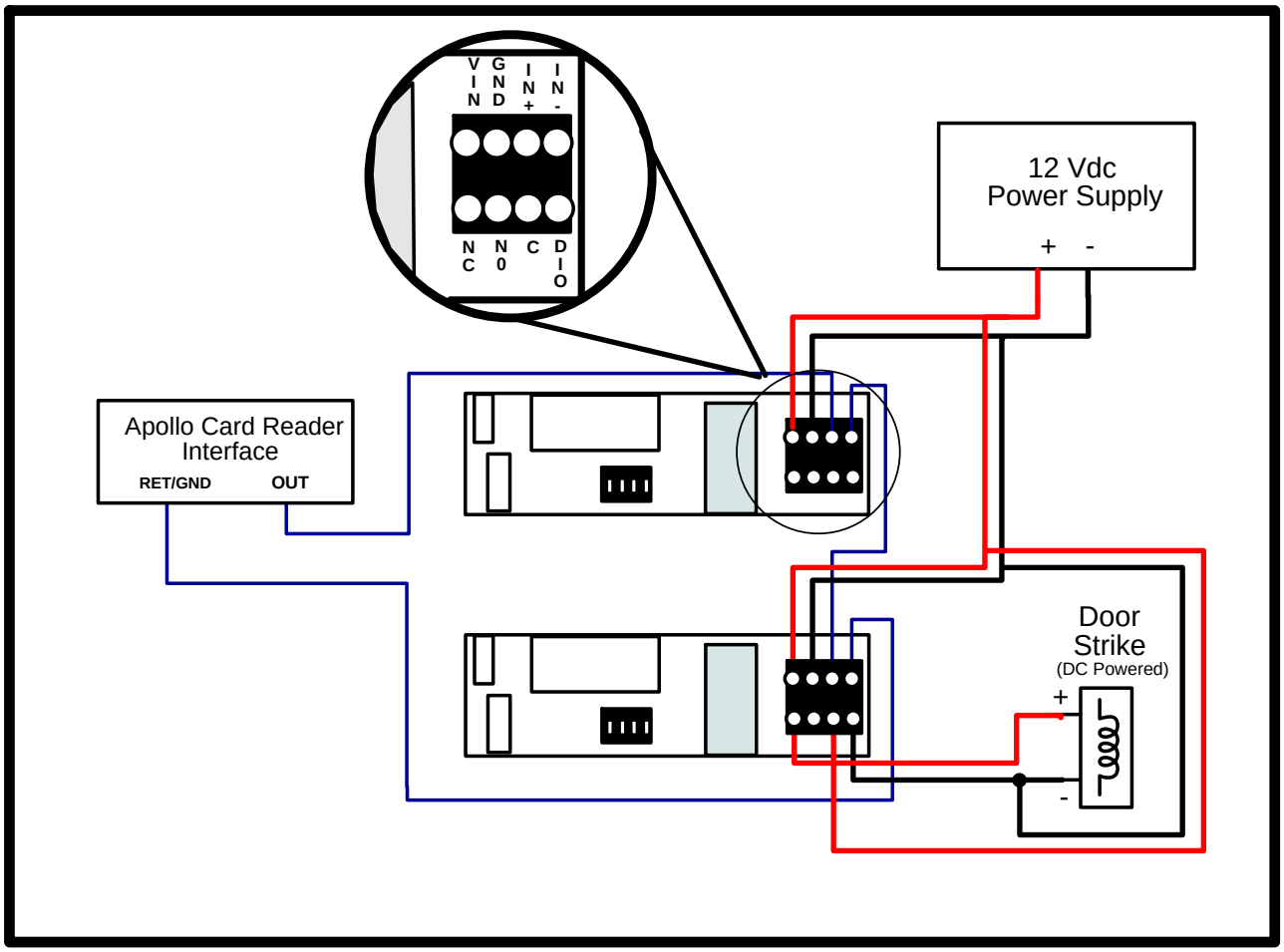


Figure 3.6.3 ADA-11 Loop and Strike Wiring. An example showing wiring with two ADA-11s with a DC Powered Door Strike. The strike is wired Fail-Secure, thus power is supplied to the strike only when the relay is activated. The ADA-10 is wired in a similar fashion but instead of wiring to terminals, wiring must be connected to the special connector of the ADA-10.

3.6.4.1 Strike Wiring, External ADA-10/11, High Security Relay

Use of the internal relays provided on the AAN-4 reader provides a possible security breach as described above. To prevent the possibility of illegally releasing the door by smashing open the reader and bypassing the internal relay, external, high security relays may be installed. The ADA-10 and ADA-11 relay module are designed for this purpose. These relays are not included with the AAN-4 and must be purchased separately.

The purpose of the ADA-10/11 high security relay is to supervise (protect) the wiring between the reader and the electric strike. IF THERE IS A POSSIBILITY OF AN INTRUDER ILLEGALLY GAINING ACCESS TO THESE WIRES, THE ADA-10/11 SHOULD BE USED. If someone illegally gains access the wires between the reader and the ADA-10/11, it is not possible to cause the door to release. The information passing along these wires is encoded, digital data, not a simple short or open circuit that is easily compromised.

The wiring between the ADA-10/11 module and the electric strike itself is not protected. To maximize the increased security of the ADA-10/11 module, the module should be mounted as close to the actual electric strike as possible, minimizing the length of the unprotected wires.

The ADA-10 module is a potted module with an 8 position connector on the end of a short ribbon cable. Optional connectors and mounting tools (ATL-10, 490-040) may be purchased from Apollo

The ADA-10 has several jumpers on the top surface that must be cut to configure the operation of the relay. When cutting the jumpers, it is important to only cut the jumpers at the top of the loop and bend the two halves apart to prevent them from touching. DO NOT CUT THE JUMPERS FLUSH WITH THE SURFACE OF THE ADA-10 AS IT MAY BE NECESSARY RECONNECT THEM LATER IF THE WRONG JUMPERS HAVE BEEN CUT. It may be necessary to wrap the ADA-10 with insulated tape to prevent the ends of the jumpers from shorting to any external metal objects.

The ADA-11 module is identical in function to the ADA-10 module. It is a smaller, non-potted circuit board that includes a plastic, “U Channel”, mounting track. Unlike the ADA-10 the power input does not have to be configured for 12 or 24 volt operation, it automatically works on 12 or 24 volts DC. Also in place of the jumpers that require cutting on the ADA-10 module, the ADA-11 has DIP switches which are easier to reconfigure if set incorrectly. Wiring is connected to the ADA-11 using screw terminal blocks instead of the special connectors utilized on the ADA-10.

BECAUSE THE ADA-11 IS A NON-POTTED MODULE, IF THE RELAY IS TO BE INSTALLED IN AN AREA OF EXTREME ENVIRONMENTAL CONDITIONS, THE ADA-10 IS A BETTER CHOICE. The ADA-11 circuit is coated with a protective, environmental seal, but it is not as well protected as the potted, ADA-10 module.

3.6.4.2 Additional Output Relay Wiring

Each reader input of the AAN-4 has the capability of controlling 3 output relays in addition to the strike relay. There are a total of five output relays available. The internal strike relay, an external strike relay, and the three extra output relays. The two strike relays (internal and external) perform the exact same functions, releasing the door when required. The extra three relays available are defined as Local Alarm, Aux Out 1, and Aux Out 2.

The function of the Local Alarm relay is pre-programmed in the firmware of the reader and cannot be modified. The reader will activate this relay whenever any of the following conditions exist:

Door Forced Open (Reader Detects the Door Contact Input Open Illegally)
Door Held Open (Reader Detects the door has not closed after legal entry)
Auxiliary Alarm (Either of the Auxiliary Alarm inputs are opened)
Reader Tamper (AAN-4 Tamper Input is opened)

Because control of the local alarm relay is completely self contained within the reader interface, this relay will activate anytime the above conditions occur, regardless of proper functioning of the other components in the system. This relay does not require communications to be working, the controller to be functioning, the PC to be operating, or the software to be running. The only thing required for the local alarm relay to operate is power (battery backed up UPS power supplies may be used). Because of this extremely reliable operation, the Local Alarm relays are often used as a redundant backup to other system functions in highly critical areas. Some typical uses for the Local Alarm relay are as a standalone siren above certain doors, connection into other alarm systems, and small bell to signal Held Open to get the people holding the door open to close it.

FOR PROPER OPERATION OF THE LOCAL ALARM RELAY, ALL UNUSED INPUTS MUST BE TERMINATED. In the Unsupervised mode, jumpers should be connected to any unused Aux Alarm or Door Contact Input. If the reader is being used in the supervised mode, 300 ohm resistors or ATM-30 terminators with a jumper between inputs 1 and 2 should be connected to all unused inputs. For information, see the section regarding input supervision.

The Aux Out 1 and 2 relays are programmable relays that require programming to configure their operation. They may be linked to other system alarms or events to trigger a siren or bell. An example may be to connect a siren to a Aux Out relay connected to a reader near the security Supervisor's office and configure the software to activate this relay (siren) whenever any door in the entire system is Forced Open. The actual capabilities of the Aux Out relays are dependant on the software system being used and the type of controller.

The use of any of these three relay capabilities requires addition of external ADA-10/11 relay modules. THESE RELAYS ARE NOT PROVIDED WITH THE AAN-4 AND MUST BE PURCHASED SEPARATELY. The ADA-10 relay module is a potted module suitable for use in areas where extreme environmental

conditions may be present, the ADA-11 is a smaller, non-potted version that should not be used in areas of extreme environmental conditions. See the above sections for more information about the ADA-10 and ADA-11 external, high-security relay modules.

3.6.4.3 ADA DIP Switches/Jumpers

In order for ADA-10 and ADA-11 devices to operate properly, The the corresponding Jumpers or DIP switches must be set in order to define the purpose the ADA will serve. First the Group identifier must be set. For the AAN-4, four group identifiers are valid:

GROUP A=Reader 1

GROUP B=Reader 2

GROUP C=Reader 3

GROUP D=Reader 4

ADA-11

On the ADA-11, addresses are set by simply pushing the switch to the correct ON or OFF position on the device.

ADA-11 Group Setting		
GROUP	S4	S3
A	OFF	OFF
B	ON	OFF
C	OFF	ON
D	ON	ON

Table 3. 6 .1: ADA-11 Group Setting

Next, the function of the ADA-11 must be defined. For each group, there are four possible settings:

ADA-11 Function Setting		
Function	S2	S1
Strike Relay	OFF	OFF
Local Alarm	OFF	ON
Aux Relay 1	ON	OFF
Aux Relay 2	ON	ON

Table 3. 6 .2: ADA-10/11 Function Setting

The above functions will work the same for each group. Thus, if group B is selected (S4=ON S3=OFF), and the function Strike Relay is selected (S2=OFF, S1=OFF), the ADA will function as the strike relay for Reader 2.

ADA-10

On the ADA-10, the jumpers must be cut using wire cutters to assign the group/function. DO NOT CUT THE JUMPERS FLUSH WITH THE SURFACE OF THE ADA-10 AS IT MAY BE NECESSARY RECONNECT THEM LATER IF THE WRONG JUMPERS HAVE BEEN CUT

ADA-10 Group Setting		
GROUP	G1	G2
A	NOT CUT	NOT CUT
B	NOT CUT	CUT
C	CUT	NOT CUT
D	CUT	CUT

Next, the function of the ADA-11 must be defined. This is done by cutting THREE of the four jumpers for Output Select on the ADA-10. For each group, there are four possible settings:

ADA-10 Function Setting				
Function	1	2	3	4
Strike Relay	NOT CUT	CUT	CUT	CUT
Local Alarm	CUT	NOT CUT	CUT	CUT
Aux Relay 1	CUT	CUT	NOT CUT	CUT
Aux Relay 2	CUT	CUT	CUT	NOT CUT

The above functions will work the same for each group. Thus, if group B is selected (G1=NOT CUT G2=CUT), and the function Strike Relay is selected (1=NOT CUT 2=CUT 3=CUT 4=CUT), the ADA will function as the strike relay for Reader 2.

For your convenience, the settings for the ADA-10 are printed on the product label affixed to the housing. It is also reproduced in Part 6 of this manual.

3.7 General Alarm Inputs

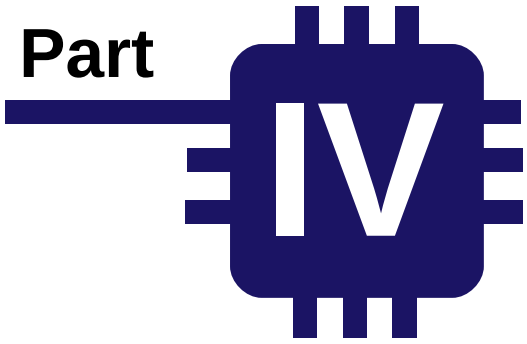
The AAN-4 provides one general alarm input. The wiring to the input should be made with twisted pair 24 AWG wire. If these input is not used, it should be 'jumpered' using a 1" (25 mm) long piece of wire connecting the two terminals to form a closed circuit. This will prevent an alarm condition being reported to the host.

3.7.1 Cabinet Tamper

This is a normally closed input and should have a jumper installed if not used!

Cabinet Tamper Input: TB19

This input is for connection to a switch located on the cabinet in which the AAN-4 is installed to detect unauthorized access to the panel. This is a normally-closed contact. In the event of a tamper condition, the exit push buttons will not function on all 4 reader connections. This condition will last until one minute after the tamper has ended. This feature restricts the ability to have easy control of all the doors by merely shorting the EPB input.



Software Configuration Utilities

APOLLO
intelligent security solutions

4 Software Configuration Utilities

The software utilities described in the following section can be downloaded from the Downloads page of the Technical Support section of the Apollo Security website.

Apollo's website can be found at **http://www.apollo-security.com**

For further questions regarding obtaining these utilities, contact your Apollo support representative.

4.1 ENI-100 IP Programming

The ENI-100 occupies one IP address in order to connect to the network and to the programming host.

The address of the ENI-100 can be set in three ways: The InitAAN software utility, the internal web pages, or the internal Telnet server. For ease of setup, using InitAAN is recommended.

In addition to IP address programming, additional security features can be enabled on the ENI-100 to protect from unauthorized use. ***The default password is blank and should be changed on first use to prevent unauthorized configuration of the device. This can be done through the Web Page or Telnet setup.*** Additional security settings can be performed via the Web and Telnet setup only. These include disabling Web Page setup, disabling Telnet setup and enhanced password. For more information see the following sections on Web and Telnet configuration.

ENI-100 Default Settings

IP Address:	**192.168.10.178**
www username:	**<blank>**
www password:	**<blank>**
telnet password:	**<blank>**
telnet port:	**9999**

4.1.1 InitAAN

NOTE: In order to use the InitAAN utility for programming the ENI, ensure that you have the latest version which is available on Apollo's website at http://www.apollo-security.com. Older versions of InitAAN may not support programming the device.

1. Run the INITAAN.EXE program. A dialog box will display instructions for programming various devices. Clicking <OK> will continue to the main screen.

2. There are two methods for programming the ENI using InitAAN. In most cases, MAC Address Selection will produce the best results.

*MAC ADDRESS SELECTION (**Preferred Method**)*

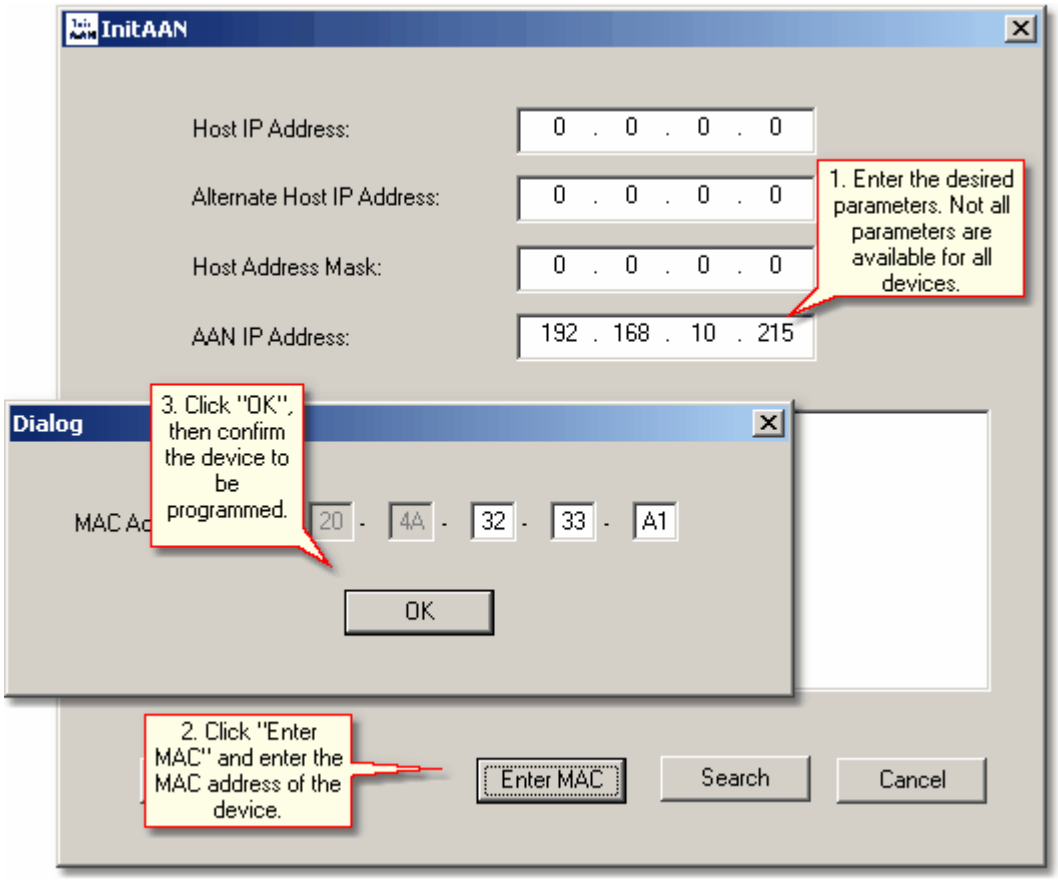
It is not necessary to use the "Search" function for this method. Depending on the network, devices that can be programmed may or may not be accessible using search.

a) First, enter the desired parameters. For the ENI-100, only the IP Address can be configured using this utility (all other parameters must be configured using the web page or Telnet). For the ENI-1 Host IP Address, Host Address Mask and Alternate Host IP address can be specified to restrict addresses that will be able to communicate with the ENI-1.

b) Click "Enter MAC" which will prompt for the MAC address of the device to be programmed. The MAC address can be found on a sticker attached to the ENI device.

c) Click "OK" and then confirm the device to be programmed. InitAAN will program the device.

d) Confirm programming by accessing the device at the new address using a web browser or Telnet (ENI-100) or using the Ping utility (ENI-100 or ENI-1).



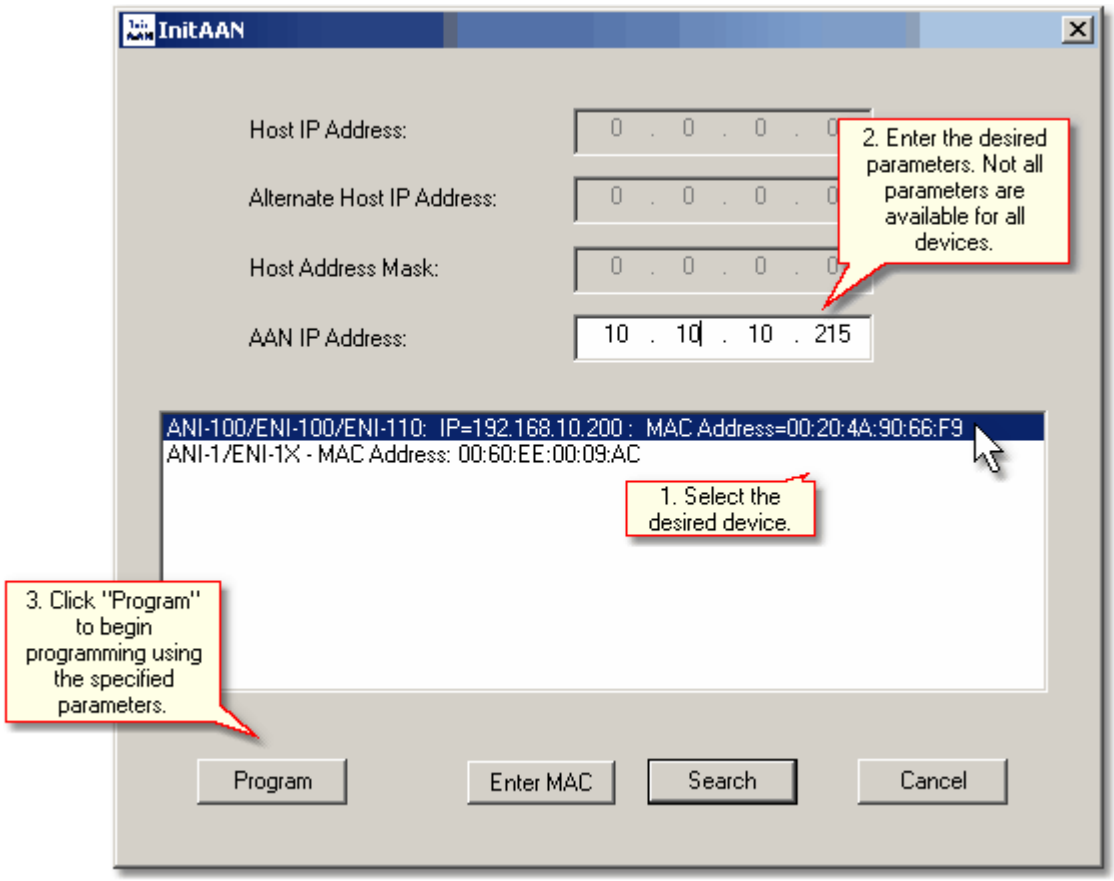
DEVICE SEARCH SELECTION

a) Click "Search" to display devices on the local network. If the desired device does not display in the list, it may be possible to program the device using the MAC Address Selection method described previously.

b) Select the device that should be programmed by clicking on it in the list. Devices can be identified by their existing IP address and/or MAC address. To positively identify a unit, compare the MAC address in the list with the address printed on the identification sticker on the device.

c) Enter the desired parameters. For the ENI-100, only the IP Address can be configured using this utility (all other parameters must be configured using the web page or Telnet). For the ENI-1 Host IP Address, Host Address Mask and Alternate Host IP address can be specified to restrict addresses that will be able to communicate with the ENI-1.

d) Confirm programming by accessing the device at the new address using a web browser or Telnet (ENI-100) or using the Ping utility (ENI-100 or ENI-1).



5. Additional devices can be programmed by repeating the above steps. To exit the program, click "Cancel".

NOTE: The PC which is running InitAAN and the network hardware (switch, router, etc) must be configured to allow network broadcasts in order to be able to communicate with the ENI and other programs to allow programming. If one or more parts of the network does not allow broadcasting it may not be possible to configure devices using InitAAN.

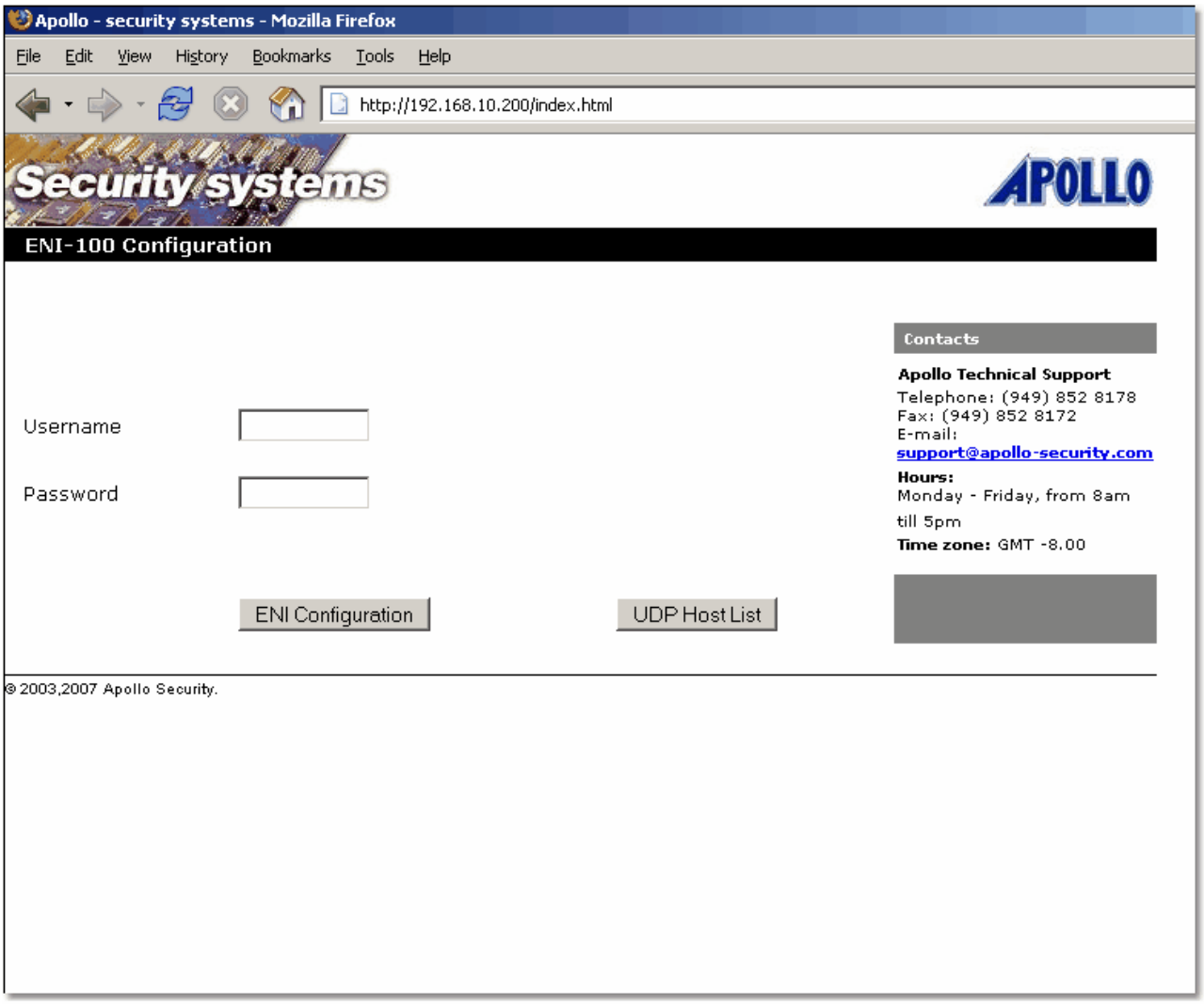
4.1.2 Web Page

In most cases, the IP address will need to be set using the configuration software as explained in the previous section. In some cases, it may be possible to use the web page for configuration, for example to make a modification to a previously configured ENI-100. *If you are unable to connect to the web page, it will not be possible to set the IP address in this manner.*

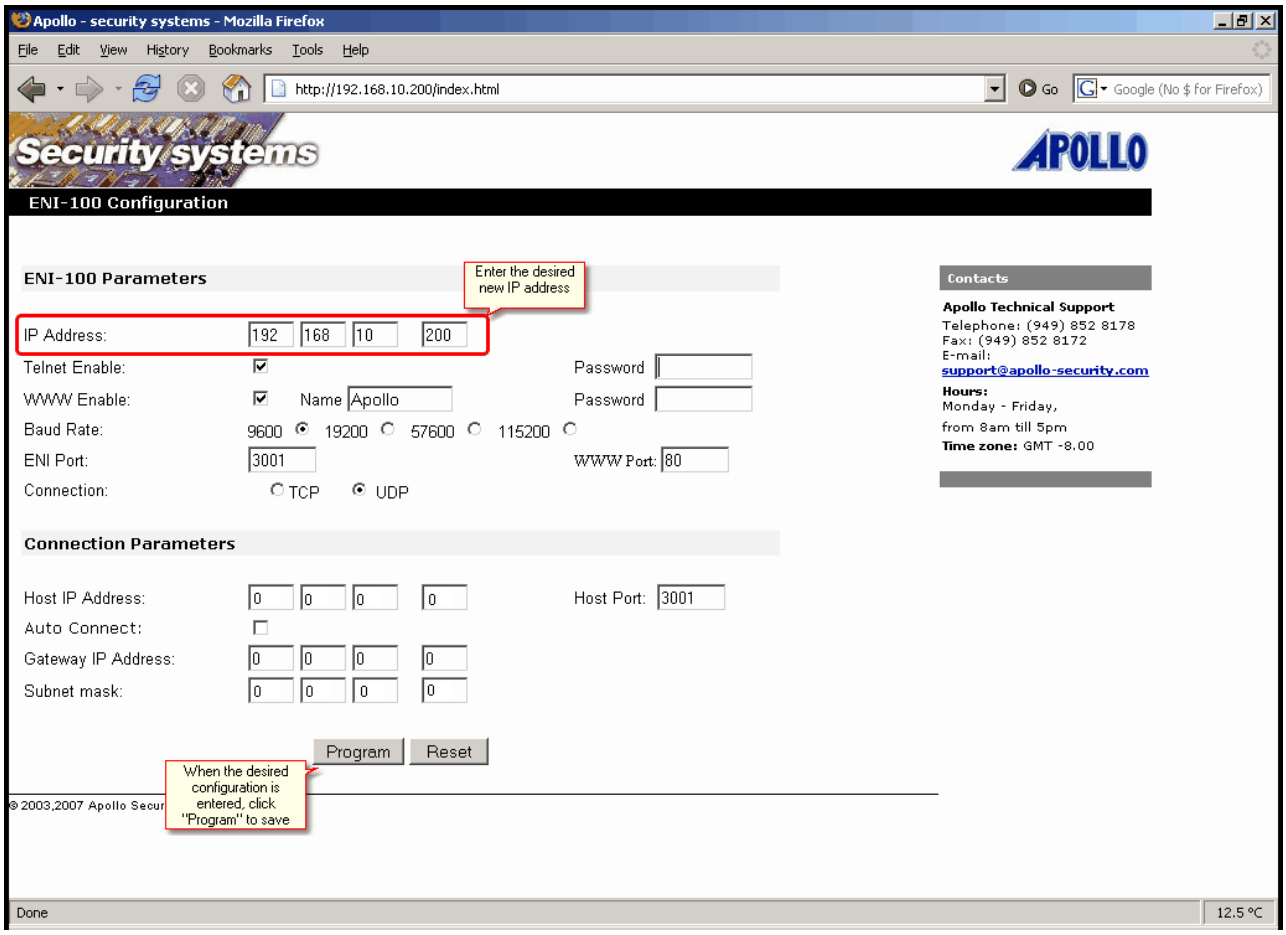
To use the web page to configure to the IP address, the IP address of your computer must be on the same network as the IP address of the ENI. For the defaults in the ENI-100 (IP Address =192.168.10.177) the computer's IP address would have to have the first 2 octets the same (192.168.x.x) for class B addresses and the first 3 octets (192.168.10.x) for class C addresses.

To change the IP address, first type the default address: "http://192.168.10.177" into the address field of your browser and press <enter> to display the login screen (see the Defaults section for default address for all devices):

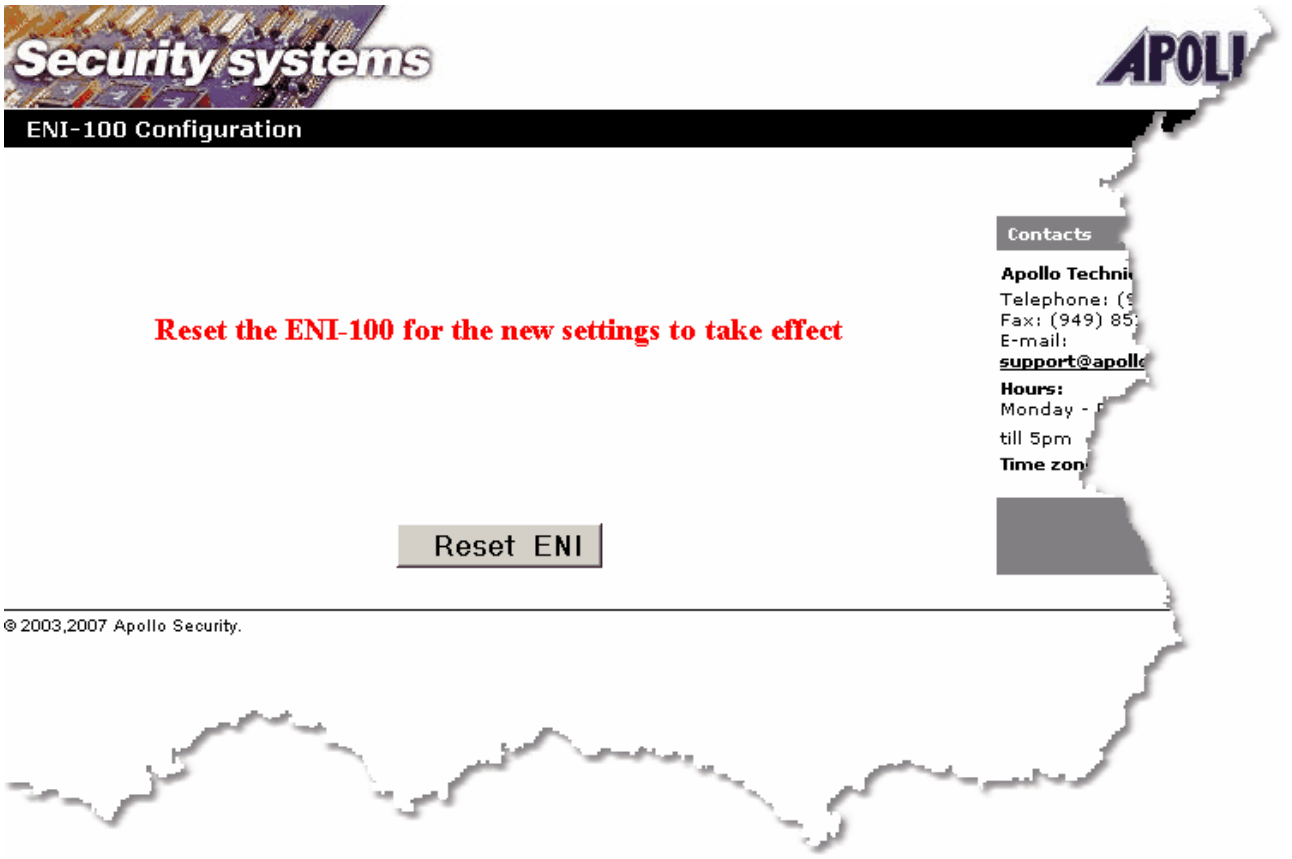
The default user name and password are blank, so unless a username/password was previously specified, simply click on "ENI Configuration" to proceed to the main configuration screen.

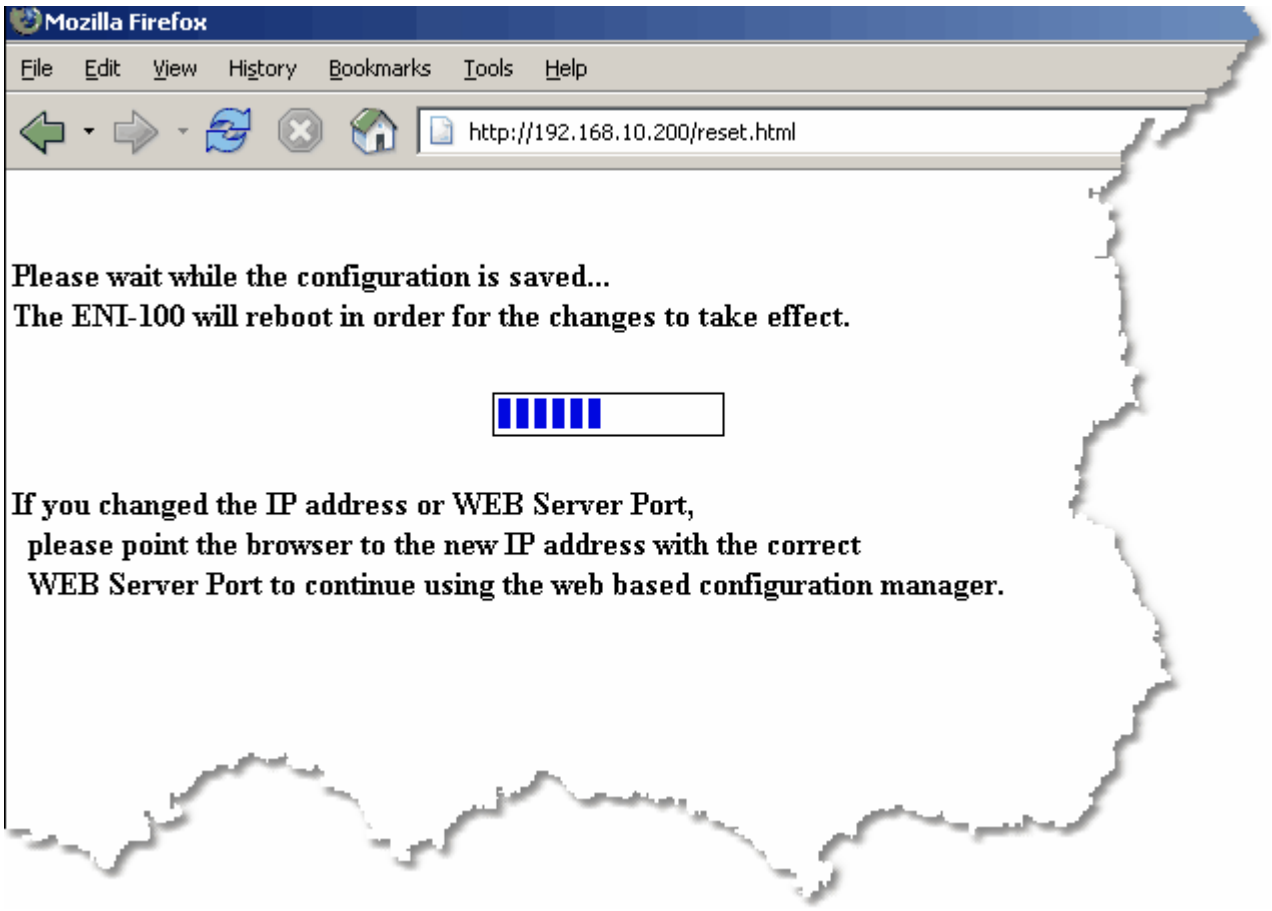


The main configuration screen shows a variety of options for the ENI-100. To change the IP address of the devices, type the desired address into the appropriate boxes. Remember that the new IP address should be available from your network in able to be able to access this web page configuration screen again. ***NOTE It is highly recommended that the default user name/password should be changed on first use to secure the device from unauthorized use!***



In order to complete the programming with new settings, it is necessary to reboot the ENI. A screen will display to allow reset by clicking the "Reset ENI" button. A status screen will be displayed while the ENI resets and when completed, the ENI will use the new settings. Note that if the IP address was changed it will be necessary to enter the new address in the browser address bar in order to access the web page configuration again.





4.1.3 Telnet

To configure the ENI using Telnet, connect to the internal Telnet server of the ENI-100 using a Telnet client using port 9999. Using the configuration menus (Menu 0 for Server Settings), change the network setup values to the desired settings.

> The correct syntax for command line telnet to access the *ENI-100* with default configuration is:
>
> *telnet 192.168.10.178 9999*
>
> This specifies to connect to address 192.168.10.178 on port 9999. Make sure to use the correct default address for your device and use a computer on the same network as the ENI.

NOTE: Once a password has been specified for Telnet access the correct password must be entered within 5 seconds of opening the telnet session or the connection will be closed. ***Passwords are case-sensitive!!***

Upon successful connection to the ENI, the current configuration will be displayed:

```
ENI-100/110
MAC address 00204A92AB82
Software version V1.02 (070416) CPK6101_XPTEX
AES Encryption
Password :-
Press Enter for Setup Mode
```

```
*** basic parameters
Hardware: Ethernet TPI
IP addr 192.168.10.215, no gateway set, netmask 255.255.255.0
Telnet config password set

***Security
SNMP is    enabled
SNMP Community Name: public
Telnet Setup is enabled
TFTP Download is  enabled
Port 77FEh is  enabled
Web Server is  enabled
Web Setup is   enabled
ECHO is    disabled
Encryption is disabled
Enhanced Password is disabled


****************Channel 1****************
Baudrate 9600, I/F Mode 4C, Flow 00
Port 03001
UDP is used.
Remote IP adr: 192.168.10.202, Port 03001
CPU performance : Standard


Change Setup:
 0 Server configuration
 1 Channel 1 configuration
 6 Security
 7 factory defaults
 8 exit without save
 9 save and exit    Your choice ?
```

The configuration can be changed by using the menu items 0, 1 and 6. After configuration has been changed, menu item 9 will exit the configuration and save changes. Selection 8 exits the configuration without saving any changes keeping the previous settings.

SECURITY SETTINGS

The following security settings can be changed only using the Telnet menu (option 6-Security). These options should be used to increase security of the ENI-100 by restricting changes to the configuration. For options, (N)=No and (Y)=Yes, pressing <ENTER> sets the default value as noted in parentheses.

Disable SNMP (N) ? - Enable/Disable Simple Network Management Protocol configuration.

SNMP Community Name (public): - Restricts the SNMP community to the specified name.

Disable Telnet Setup (N) ? - Enable/Disable Telnet setup (takes effect after saving changes and exiting the current telnet setup session).

Disable TFTP Firmware Update (N) ? - Enable/Disable firmware update by TFTP

Disable Port 77FEh (N) ? Enable/Disable detection port for the configuration software. If disabled, the software will not be able to auto-detect the device.

Disable Web Server (N) ? - Enable/Disable web configuration pages.

Disable Web Setup (N) ? - Enable/Disable configuration by web pages.

Disable ECHO ports (Y) ? - Enable/Disable echo of characters received on the serial port.

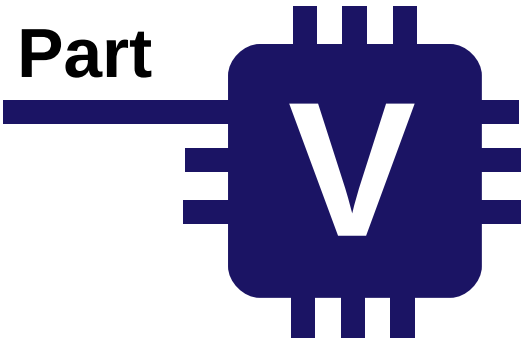
Enable Encryption (Y) ? - See *Encryption Configuration*

Key length in bits (128): - See *Encryption Configuration*

Enable Enhanced Password (N) ? - Enable/Disable 16 character password support. If disabled, the password length will only be 4 characters.

Disable Port 77F0h (N) ? - Enable/Disable advanced configuration port.

NOTE: If Telnet Setup, Web Server/Setup and Port 77FEh are all disabled, remote configuration will be completely disabled and no changes can be made to the device settings!! Configuration will only be able to be changed by resetting the device.



Troubleshooting

APOLLO
intelligent security solutions

5 Troubleshooting

5.1 Communications

The first thing that must be verified at the card reader is the RS-485 or network communication. If the controller is unable to communicate with the programming host, most other functions will not work. Communications should be verified observing the port activity LED (D15), which will blink when communication is active (see Part 2.4). If network communication is used, pinging the device from the host will determine if the network is correctly configured.

5.2 Reader / Keypad

The reader function can be verified after communications are functioning properly. The host system must be configured for each of the readers on the AAN-4 to be used, and with the correct card format. The card format is determined by the actual cards that will be used. After configuring the card format at the host, placing a card in front of the reader should generate an access message on the host computer. If the message is “Access Denied” the reason for the message will indicate further steps to be performed. “Access Denied – Wrong Facility Code” will also display the actual facility code on the card. This information should then be entered to the host computer system. “Access Denied – Not in File” will display the actual card number of the presented card. This card should then be added into the employee database of the host system.” Access Denied – Access Level Error” indicates that the cards is entered into the system but the Access Level assigned to the card does not allow access to the particular door at this time.

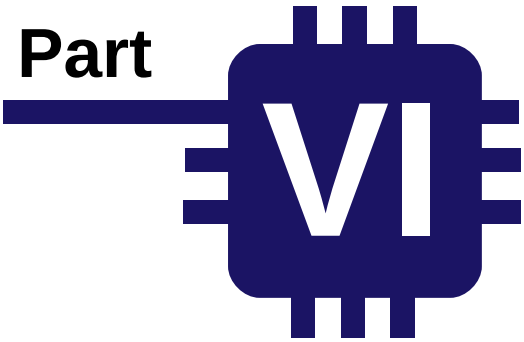
On readers with integral keypads, the keypad may be verified by setting the reader into the Card and PIN mode. After presenting a valid card, the reader should flash the yellow LED (if installed reader supports 3 color LEDs). This indicates the reader is waiting for a Pin entry. Enter a valid PIN using the keypad and press the “ENTER” key. Access should be granted.

5.3 Input Zones

All alarm inputs should next be verified. Opening the Door Contact input should generate an immediate “Forced Open” alarm. Closing the Exit Pushbutton input should release the strike relay. NOTE: the Exit Pushbutton input will not function if the reader interface is in tamper (Tamper Contact=Open) and also one minute after the tamper condition is secured. The reader may also be configured (via the host) to not activate the strike relay when the Exit Pushbutton is depressed. In all cases the reader should not report “Forced Open” immediately after pressing the Exit Pushbutton. The Aux Alarm inputs (if used) can be verified next. Some system will not allow use of the second Aux alarm. Opening the Aux alarm input should result in a message on the host system. Unused Aux alarm inputs should be terminated.

5.4 Output relays

The internal strike relays should energize any time a valid card (or PIN) is presented and the message “Access Granted” appears on the host. The reader may be set to the “Unlocked” mode at the host to permanently energize the relay for test purposes. Any external, high-security, ADA-10.11 relay modules should also be verified.



Specifications

APOLLO
intelligent security solutions

6 Specifications

Relay Specifications:

Coil: 12Vdc
Contacts: 2A @ 24Vdc
0.5A @ 125Vac

Power Requirements:

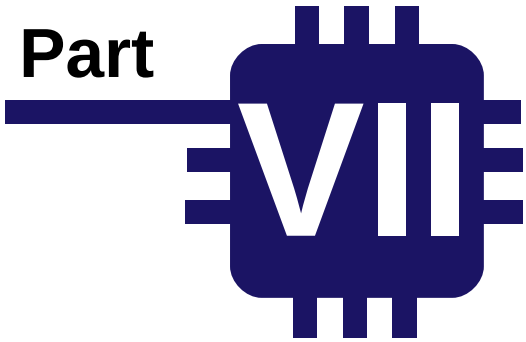
+12 to +24Vdc @ 250mA

Dimensions:

7.5 in x 5.5 in (19 x 14 cm)

Environment:

Operating Temperature:	-0 to 50° C
Storage Temperature:	-40 to 85° C
Relative Humidity:	0 to 95%, non-condensing



Supplemental Figures

7 Supplemental Figures

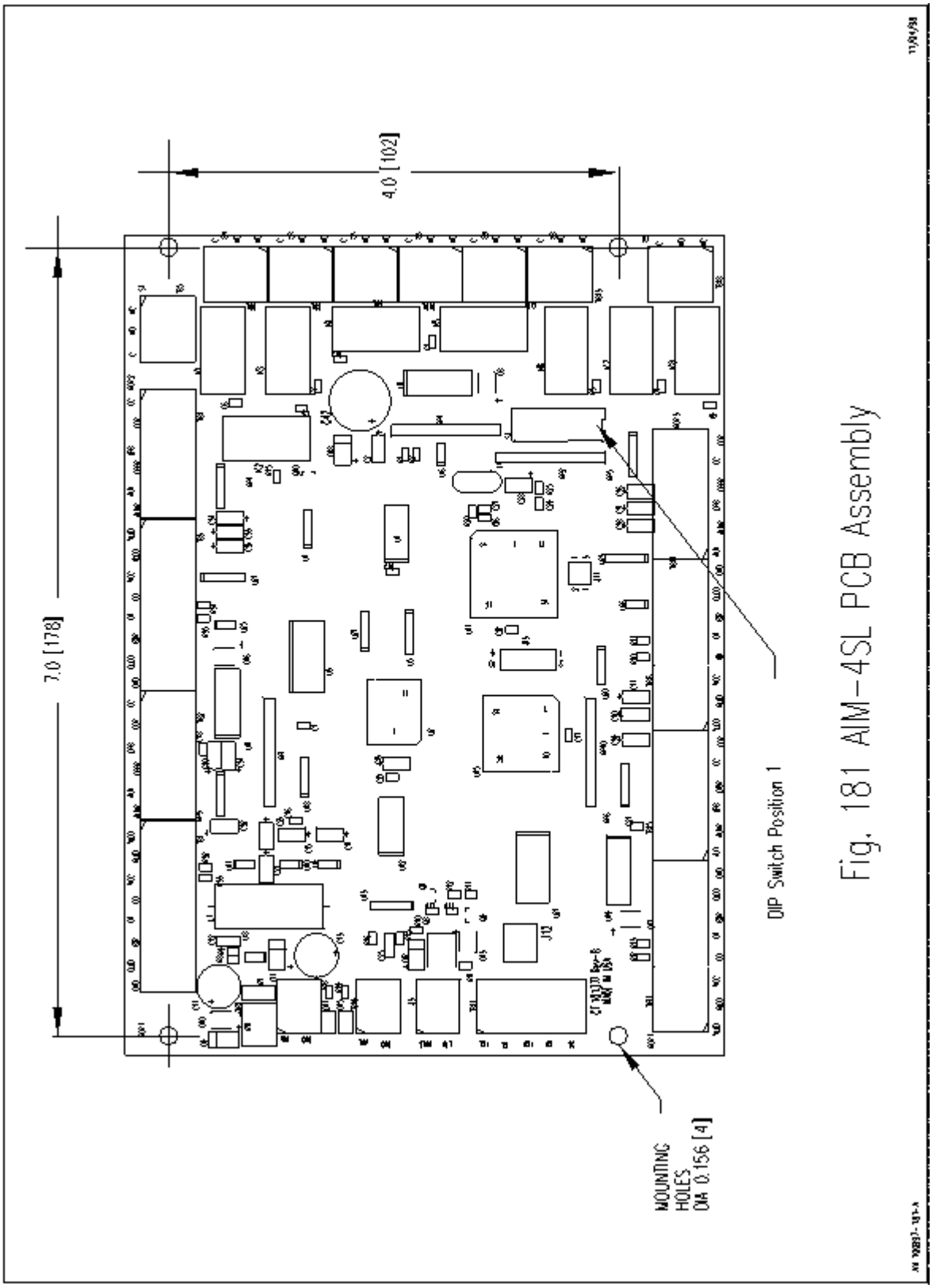


Fig. 181 AIM-4SL PCB Assembly

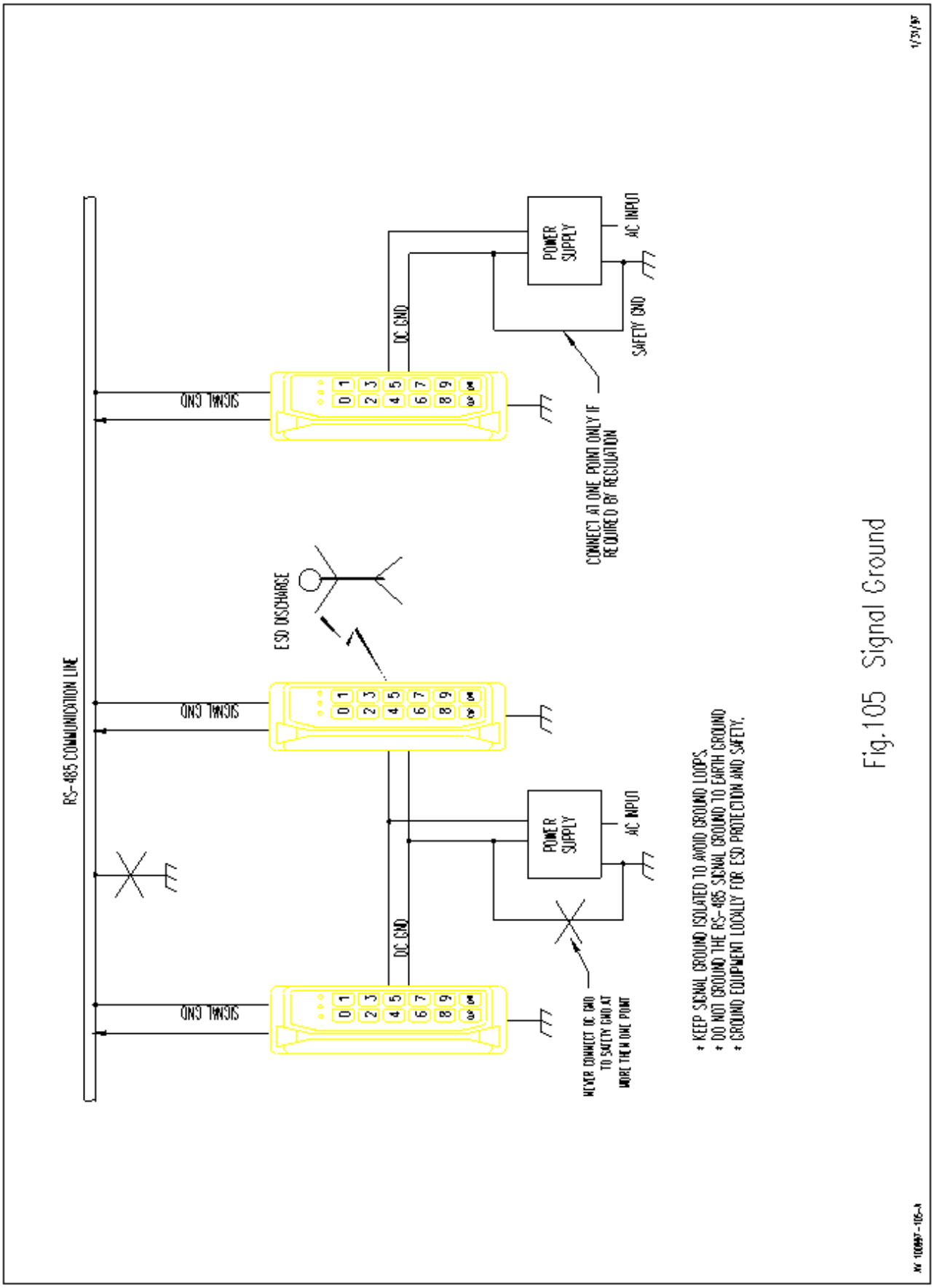


Fig.105 Signal Ground

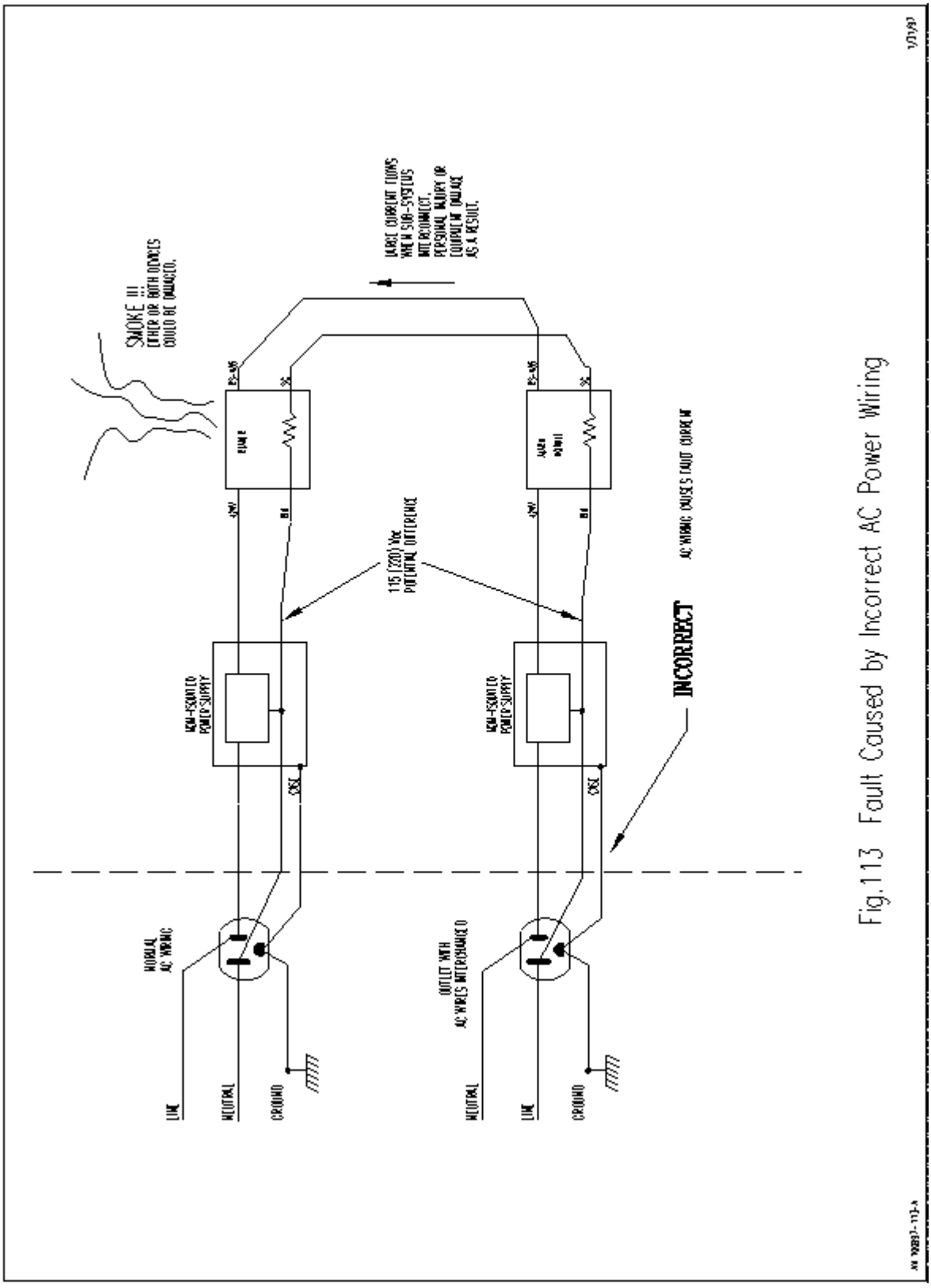


Fig.113 Fault Caused by Incorrect AC Power Wiring

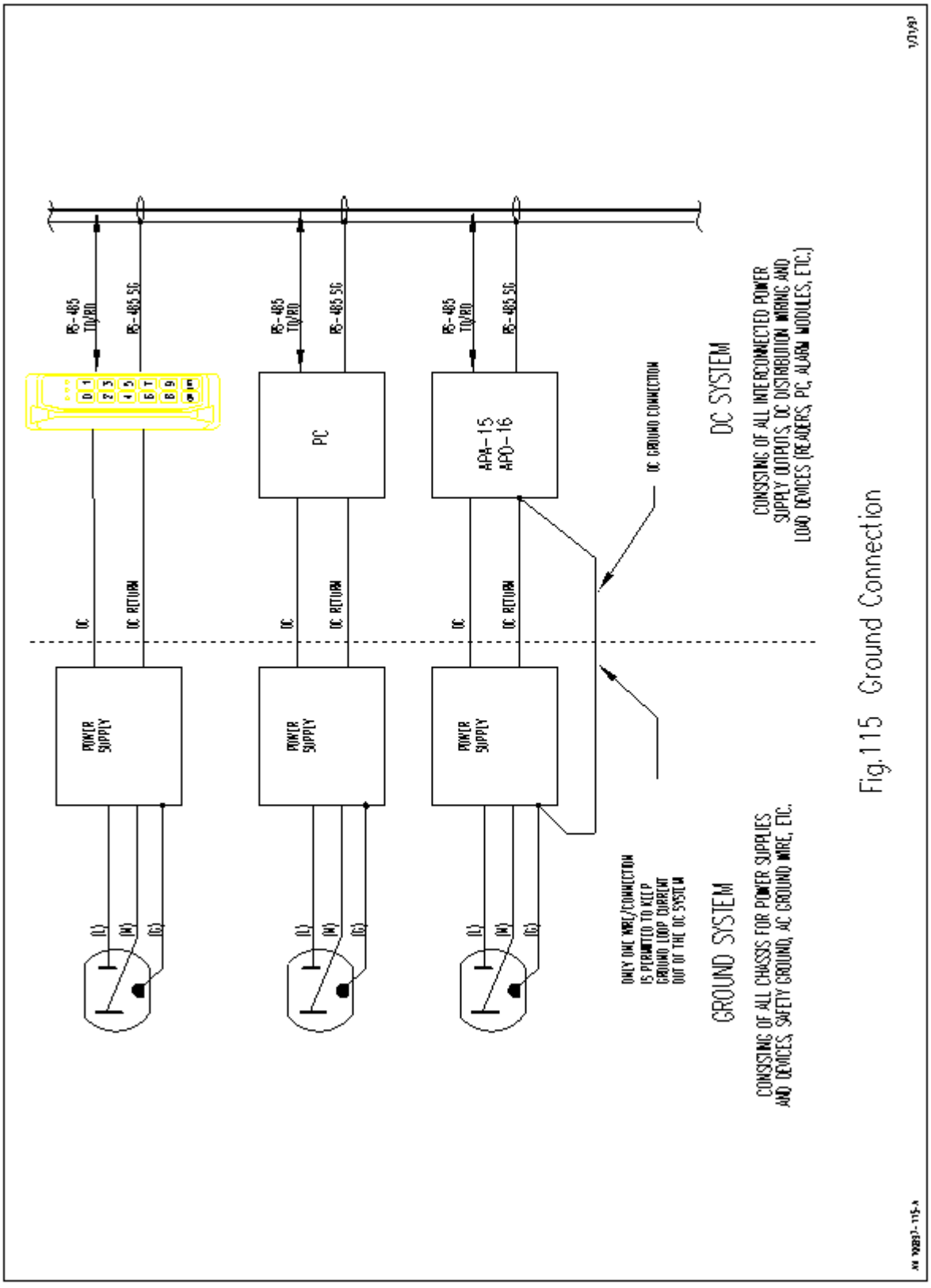


Fig.115 Ground Connection

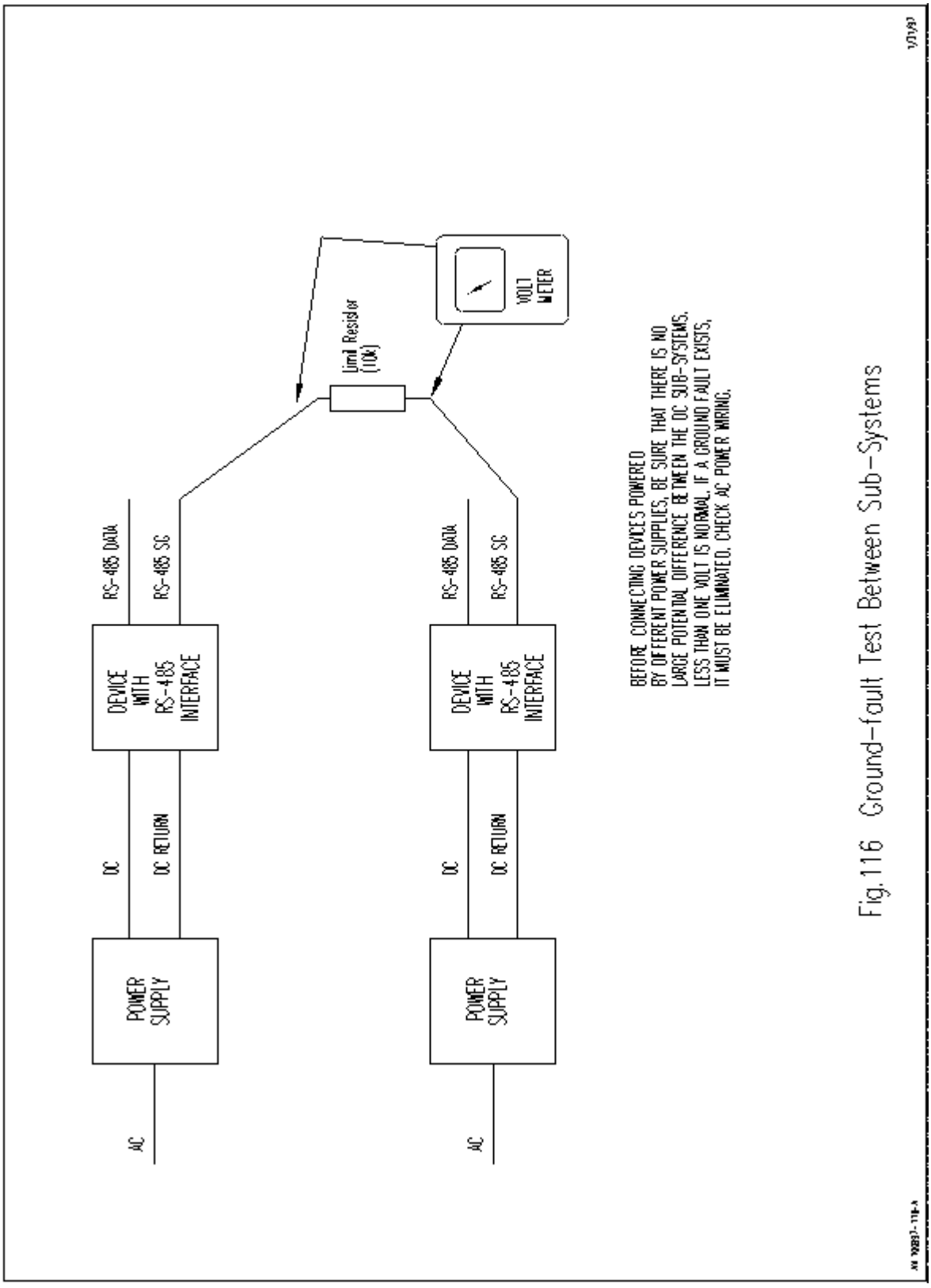


Fig.116 Ground-fault Test Between Sub-Systems

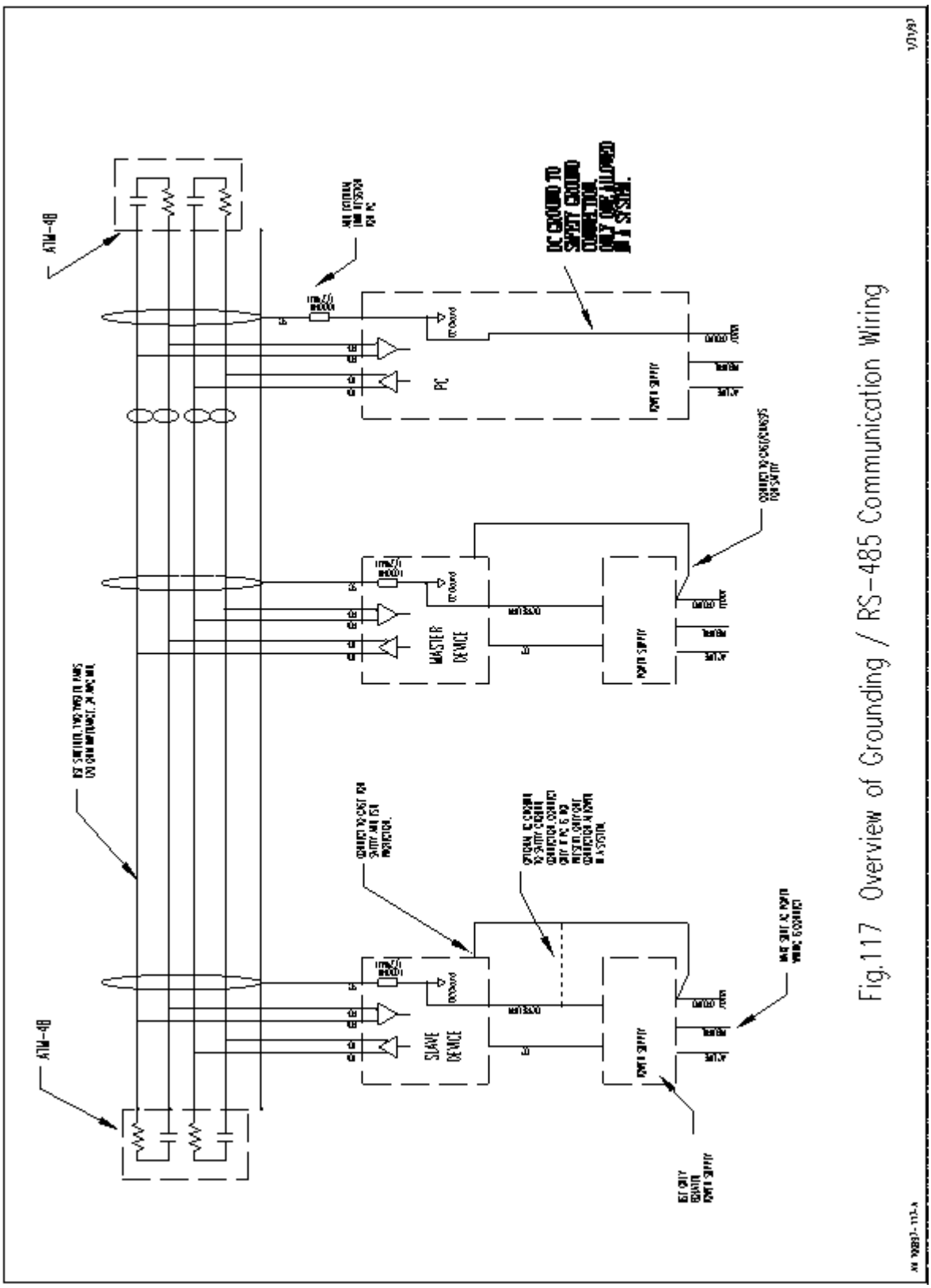


Fig.117 Overview of Grounding / RS-485 Communication Wiring

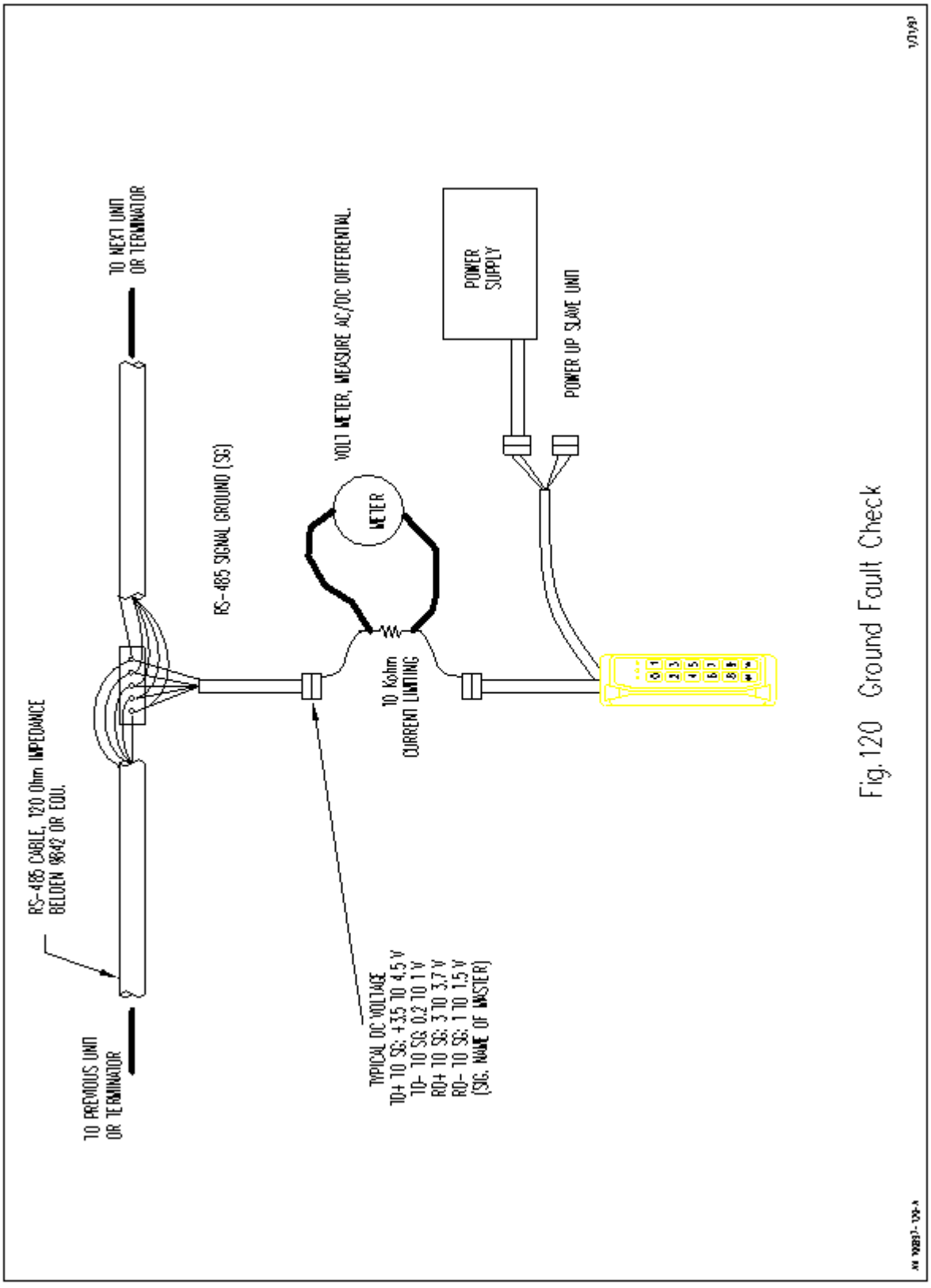


Fig. 120 Ground Fault Check

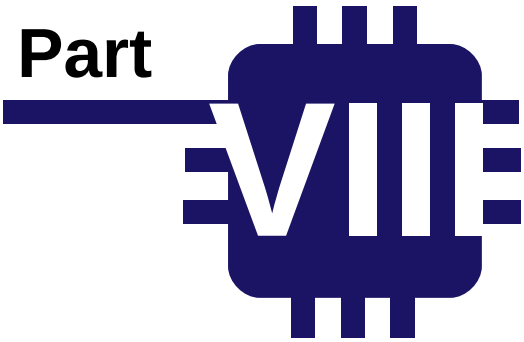
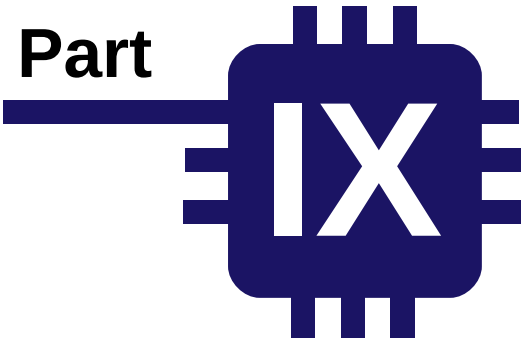


Table of Figures

8 Table of Figures

Number	Description	Page
2.1	AAN-4 Diagram	6
3.3.1	Host to AAN-4 wiring (RS-232)	18
3.2.6.1	ENI-100 Hardware Layout	19
3.5	AAN-4 Card Reader & Input Wiring	25
3.6	Input Supervision	27
3.7.3.1	Strike Wiring - Fail Secure	30
3.7.3.2	Strike Wiring - Fail Safe	31
3.7.3	ADA-11 Loop and Strike Wiring	32
181	AAN-4 PCB Assembly	52
105	Signal Ground	53
113	Fault Caused by Incorrect AC Power Wiring	54
115	Ground Connection	55
116	Ground Fault Test Between Sub-systems	56
117	Overview of Ground / RS-485 Communication Wiring	57
120	Ground Check	58



Revision History

APOLLO
intelligent security solutions

9 Revision History

REVISION HISTORY

Revision	Date	Description of changes	Editor
A	29 SEP 2007	Initial Release	R. Burnside
A.1	23 MAR 2009	Update screenshot for ENI Config (Part 3.2)	R. Burnside
A.2	25 AUG 2010	Update ADA11 switch settings; Add mounting holes diagram	R. Burnside

Index

- A -

AC power system 18
Access Control 2
ASM-23 12
ASM-48 12

- B -

Battery 13
Baud Rate 11

- C -

Capacitor (Memory Backup) 13
Connectors 11, 21

- D -

DC ground 17
Dimensions 50

- E -

ENI-100 20
Error codes 12

- F -

Firmware 13

- G -

Gateway 22
Ground connections 17
  Faults 17, 18
  Saftey (Earth) Ground 18

- H -

Heartbeat 13
Host Communication Connection 18
Host List 22

- I -

IP Address 22, 37
Isolation (Power) 17

- L -

LEDs 6, 12, 19, 24, 48

- M -

Memory Backup 13

- O -

On-board memory 13
Operating Environment 50

- P -

Power supply 17

- R -

Routing 20
RS-232 19
RS-485
  Device Drivers (ASM-48) 12
  Signal Ground 17

- S -

Self Test 12
Specifications 50
Start Up Mode 12
Supervision (Input) 26

- T -

Terminal Connectors 6