Access Easy Controller 2.1

APC-AEC21-UPS1 | AEC-AEC21-EXT1

BOSCH

en Hardware Manual

Table of Contents

1 Before You Begin

1.1 General

Access Easy Controller is a web based security system that allows you to control and monitor access routes with flexibility and conveniences to suit individual needs.

This hardware manual helps you understand the Access Easy Controller 2.1 and helps the system serve you better. Access Easy Controller is a solution invented for life.

1.2 Terminologies

The Access Easy Controller 2.1 Hardware Manual contains detailed information and connection diagrams for Access Easy Controller 2.1, its components, and peripheral field devices.

The following terminologies are used to describe the components and peripheral field devices in Access Easy Controller 2.1 Hardware Manual.

Terminology	**Descriptions**
Access Easy Controller 2.1 (hereinafter will be referred as “AEC2.1”)	Access Easy Controller 2.1 enclosure with PSU, CPU board and an Interface board (4-Reader board).
Access Easy Extension Unit (hereinafter will be referred as “Extension Unit”)	Access Easy Controller 2.1 enclosure with PSU and space for 2x interface boards (4-Reader or 8-Input-Output board) and a backup battery.
4-Reader Board (hereinafter will be referred as “4-Reader board”)	Interface board for Access Easy Controller 2.1 and Extension. The board supports 4 Wiegand readers and provides 8 input and 8 output connection ports for door control.
8-Input-Output Board (hereinafter will be referred as “8-IO board”)	Interface board for Access Easy Controller 2.1 and Extension. It supports 8 inputs and 8 outputs, fitting parts.
CPU Board	Access Easy CPU board. The CPU is the main controlling devise in Access Easy Controller 2.1 system.
Power Supply Unit (hereinafter will be referred as “PSU”)	The Power Supply Unit used in Access Easy Controller 2.1 has an input power of 100~240 VAC.
EM Reader	Access Reader 8000 Wiegand EM Prox.

2 Overview of Access Easy Controller 2.1

2.1 Architecture of Access Easy Controller 2.1

The basic architecture of an AEC2.1 system can be divided into two main building blocks, namely the Power and the Function. The Power block provides the required power to all the modules and sustains the system in times of AC power failure. The electrical input sources vary according to individual electrical power standards in the country.

The Function block can be divided into three different modules namely the Software, the Processor and the Interface module. These modules work together to define the system’s characteristics and behaviors. Interactions between the modules are carried out through standard RS232 and RS485 channels. Such architecture structure allows versatilities in system designing and building.

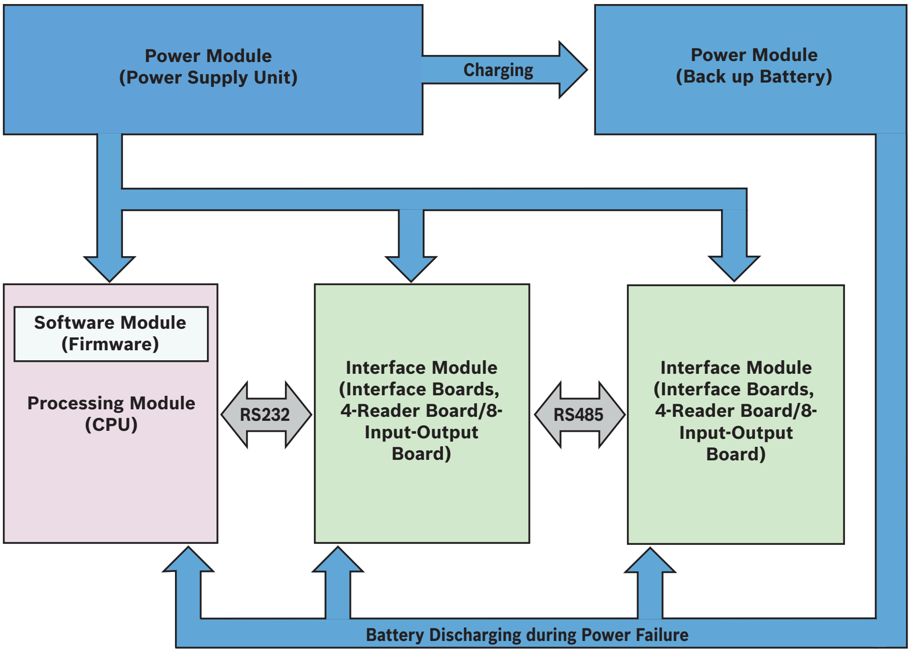


Figure 2.1 Access Easy Controller 2.1 Architecture

2.2 Basic Functions in Access Easy Controller 2.1

Based on hardware configuration and database setup, AEC2.1 offers all the features and functions available with high-end access controllers.

- Door access control using card readers, or card reader and PIN code
- In and Out readers for high security areas
- Video verification for door access
- View Live and Playback videos
- Download event videos to PC
- Anti-passback control
- Alarm monitoring of reader controlled doors for Door Held and Door Forced conditions
- Alarm monitoring of non-reader doors and other inputs
- Manual door unlocking and locking
- Automatic door locking and unlocking based on schedules
- Automatic Arming and Disarming of input points

- Lighting and output control based on schedules
- Special scheduling option for holidays
- Built-in reporting capabilities
- Common alarm output for connection to intrusion alarm system

AEC2.1 supports a wide range of applications, it is necessary you understand how to configure it and select the necessary hardware, such as card readers or additional input/ output boards.

Unlike other access controllers, no special software is required on a host computer. The software needed to program and operate the AEC2.1 is built in the controller. Data entry and system monitoring functions are performed by connecting to the controller with a standard Web browser, such as Microsoft's Internet Explorer version 7.0.

For more information on using the data entry and monitoring screens, refer to the AEC2.1 Software Manual.

2.3 Basic Access Easy Controller 2.1

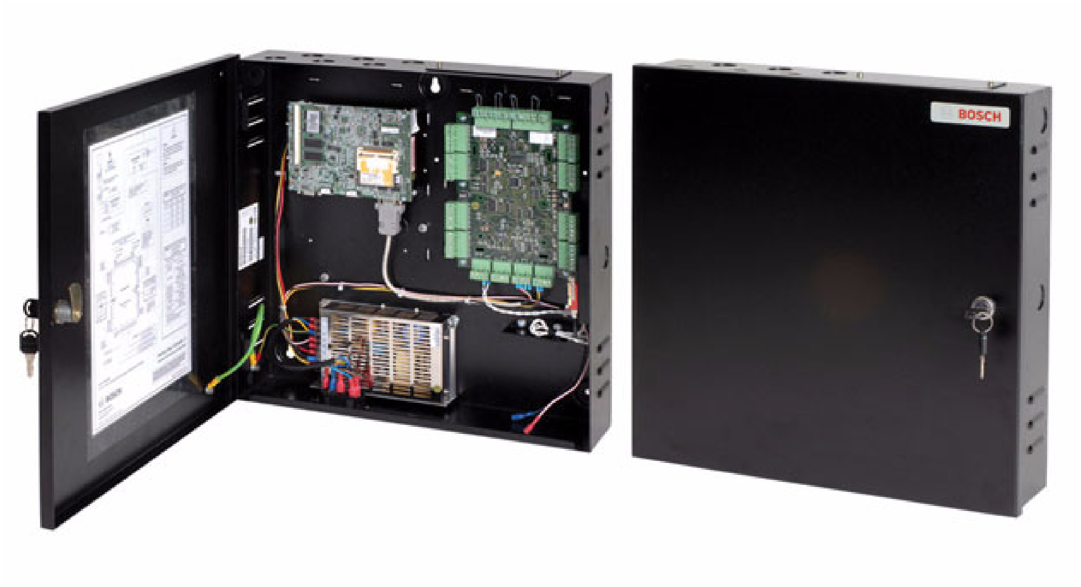


Figure 2.2 Access Easy Controller 2.1

The basic AEC2.1 system consists of a single metal enclosure with three components: **CPU**, **4-Reader board**, and **Power Supply Unit (PSU)**. Space is provided for a 12-volt standby battery to sustain the system in time of power failure. The PSU in the controller has an input power of 100~240 VAC. The enclosure is key locked and is equipped with a tamper switch to detect any tampering of the panel, and/or when the controller door is being opened.

In its minimum configuration, an AEC2.1 system supports one 4-Reader board. The board comes with, 4 card reader, 8 input, and 8 output ports to support all necessary hardware (door lock/strike outputs, door contact inputs and request-to-exit inputs). A full AEC2.1 system supports up to a maximum of 16 interface boards (eight 4-Reader boards and eight 8-IO boards). This allows the AEC2.1 system to support up to 32 card readers, 64 alarm type input and 64 controllable output points.

CPU Board - The CPU board contains a microprocessor, RAM memory and all necessary electronic circuitry to interact with other circuit boards. The CPU board also contains the hardware and software needed to interface to an Ethernet-type network and to communicate with host computers using TCP/IP protocol.

4-Reader Board - The 4-Reader board is an interface board for AEC2.1. The reader board contains all circuitry necessary to interface with, and operate, up to four card readers. The reader board also provides wiring termination points for the readers, door strikes or magnetic locks, door contacts and request-to-exit devices. The first interface board of the system communicates with the CPU board via the RS232 channel. The subsequent interface boards are linked through a multi-drop communication channel, RS485, to form the system. The PSU supplies the required power to the board.

8-Input-Output Board -The 8-IO board is an interface board for AEC2.1.The 8-IO board provides the necessary circuitry to monitor 8-alarm type (non-reader) inputs, and to control up to eight external devices, such as bells, fans, lights, etc. The board also provides wiring termination points for the input and output devices. The first interface board of the system communicates with the CPU board via the RS232 channel. The subsequent interface boards are linked up through a multi-drop communication channel, RS485. The PSU supplies the required power to the board.

Access Easy Extension - Access Easy Extension is a metal enclosure identical in size to the basic AEC2.1. The Extension unit contains a Power Supply Unit, and space to install up to two additional 4-Reader boards and/or 8-IO boards. Space is provided for an optional 12V, 7AH standby battery to sustain the system in time of power failure.

NOTICE!
AEC2.1 does not come with the 12 VDC standby battery. Refer to *Section 20 Appendix D Selecting A Correct Battery Size* in this manual for backup battery specifications.

3 System Layout

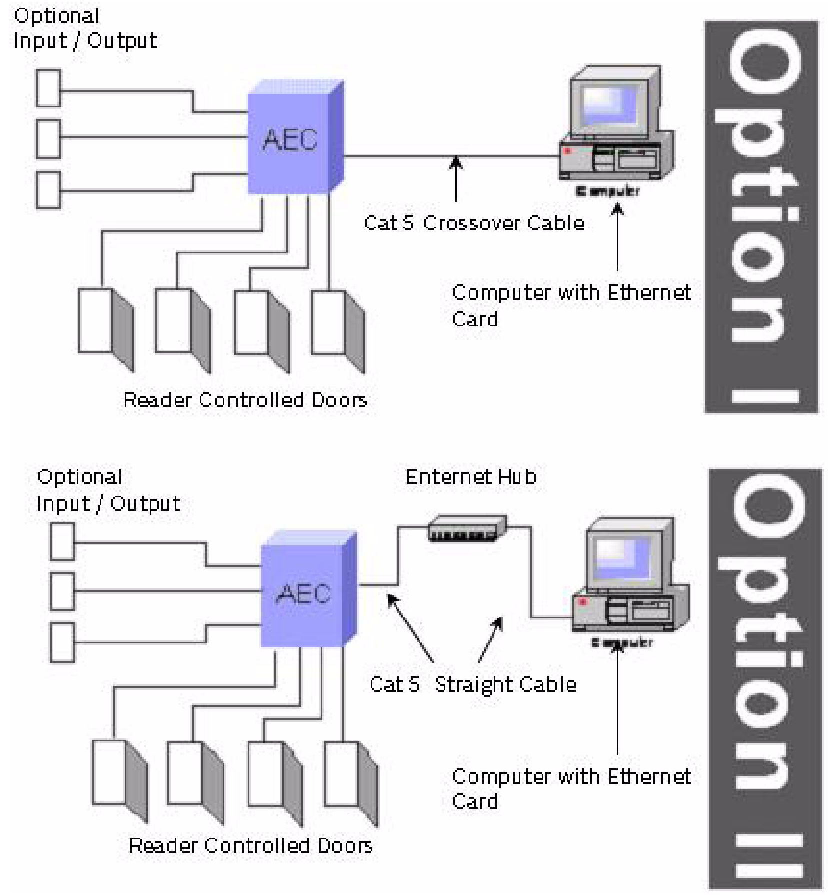


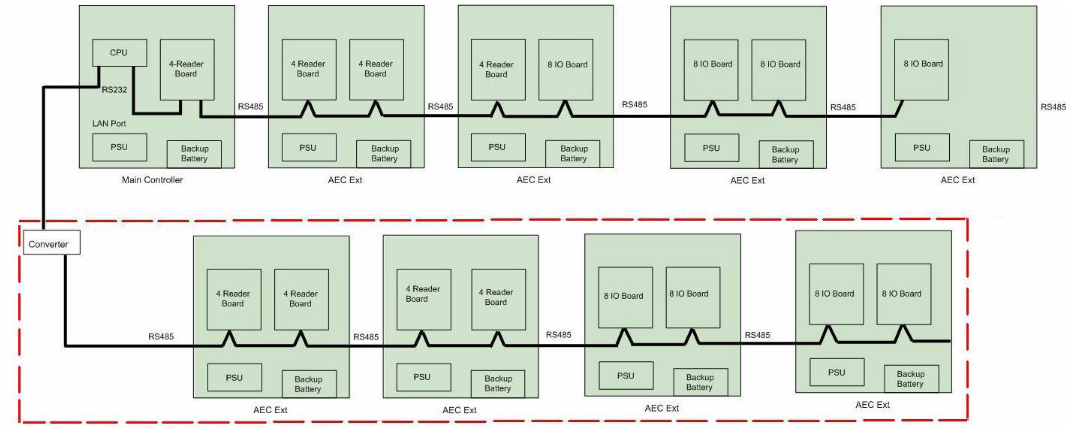
Figure 3.1 System Layout

Each AEC2.1 system can support up to a maximum of 16 interface boards (eight 4-Reader boards and eight 8-IO boards). This configuration allows the system to support up to 32 Wiegand readers, 64 alarm type inputs and 64 controllable output points. System configurations may vary, based on the requirement of the customer.

Note: UL listed panic hardware shall be used for the applications.

The figure below shows a basic configuration of the AEC2.1 system (including the converter and additional four 4-Reader boards and four 8-IO boards).

Figure 3.2 shows the basic configuration of AEC2.1 system with additional four 4 -Reader boards and four 8-IO boards using a converter. The converter UDS1100 can be linked to AEC2.1’s CPU LAN port through an ethernet network port to provide an additional multidrop communication channel upgrading it to support up to a maximum of 16 interface boards (eight 4-Reader boards and eight 8-IO boards). This allows the AEC2.1 system to support up to 32 card readers, 64 alarm type input and 64 controllable output points.



8X4-Reader Board = 32 Readers (64 programmed Inputs and Outputs)
8X8 Input/Output board = 64 Inputs & Outputs (free programmable I/O)
Each RS 485 loop can support upto 4X4 reader board and 4X8Input/Output board

Figure 3.2 Basic Configuration of AEC2.1 system

3.1 System Specifications

Dimensions

Enclosure (H x W x D)	:	400mm x 400mm x 94mm

Controller

CPU	:	32 bits Microprocessor 500 MHz or higher
Memory	:	128 MB RAM or higher
Storage	:	Compact Flash 256 MB and above
Data Integrity	:	Encryption used for user ID and PIN

Power Requirements

Primary Voltage Input (AC)	:	100~240 VAC
Secondary Voltage Input	:	+5 VDC for CPU board +13.6 +/-0.1 VDC for 4-Reader and 8-IO boards
Backup Battery	:	12 VDC, 7 AH rechargable battery

(Optional: Not included in standard package)

Interface Boards	:	4-Reader Board	8-IO Board
Voltage Requirement	:	+13.6 +/-0.1 VDC from PSU	+13.6 +/-0.1 VDC from PSU
Number of Wiegand Readers Supported	:	4	-
Number of Monitoring Points	:	8*	8
Number of Output Control Relays	:	8**	8

NOTICE!
* Input Monitoring Points on the 4-Reader board consist of door contact input and request-to-exit inputs associated with reader-controlled doors.
** Output Control Relays on the 4-Reader board are the door strike/magnetic lock control relays for the reader-controlled doors.

Readers Supported by AEC2.1

Standard Wiegand I/P Reader	:	HID MiniProx Reader, HID ProxPoint Reader, HID ProxPro with/without Keypad Reader, HID iCLASS with/without keypad Reader (R10, R30, R40)

Ports

LAN Ports	:	Two RJ45
Serial Ports	:	Two RS232
Extension Ports	:	One RS485

AEC2.1 Capacity

Number of Concurrent Logins	:	8	
User Licenses	:	Max. 25 user account (including “superuser”), using up to 50 characters, alphanumeric, case sensitive user IDs and passwords	
Database Integrity	:	Encryption used for user IDs and PINs	
Number of Cards Supported	:	20,480	
Number of Access Groups	:	254	
Number of Time Schedules	:	255	
Interval per Time Schedules	:	Four intervals per day, plus holidays support	
Recommended Web Browser	:	Microsoft Internet Explorer version 7.0 or above	
		4-Reader board	8-IO board
Max. Number of Interface Board Supported in a Full AEC2.1 Configuration	:	8	8
Max. Number of Wiegand Reader Supported in a Full AEC2.1 Configuration	:	32	-
Max. Input Supported in a Full AEC2.1 Configuration	:	-	64 (Both normally opened and normally closed devices supported)
Max. Output Supported in a Full AEC2.1 Configuration	:	-	64 (Form-C PCB mounted output control relays, with Contact Rating: 1A @ 24 VDC)

Environment Conditions

Temperature (Operating)	:	0 to +50 deg.C (32 to 120 deg.F)
Relative Humidity	:	10% to 85% (+/- 5%) at 32 d eg.C (+90 deg.F)

Certifications and Approvals

Certifications, Approvals, and Safety Standards that AEC2.1 comply with	:	CE, FCC

4 The CPU Board

This chapter provides a brief overview of the AEC2.1 CPU board. This chapter also describes the board layout and functions of various circuits. Some major components of the board are explained and information concerning jumper option is provided.

The AEC2.1 CPU board is X86 processor based Single Board Computer (SBC) with one or two 100Base-T Ethernet. The serial port (RS232), communicates with the 4-Reader and/or 8-IO boards.

The CPU board is designed to function as an embedded Web server and an AEC2.1 system.

Two communication ports are available on the CPU board. The first is an 100Base-T Ethernet port used by the Web server to communicate with the customer's database management computers. The Ethernet port terminates in an RJ-45 jack located on the CPU board. Standard category 5 cable is used to connect from the RJ-45 jack to a hub or wall outlet on the customer's network. Alternatively, a cross-over cable can be used to connect from the Ethernet jack on the CPU board directly to the Ethernet connector on the customer's computer.

The second communication port is a RS-232 port. This port is used to connect to an external modem to allow dial-in connection to the controller.

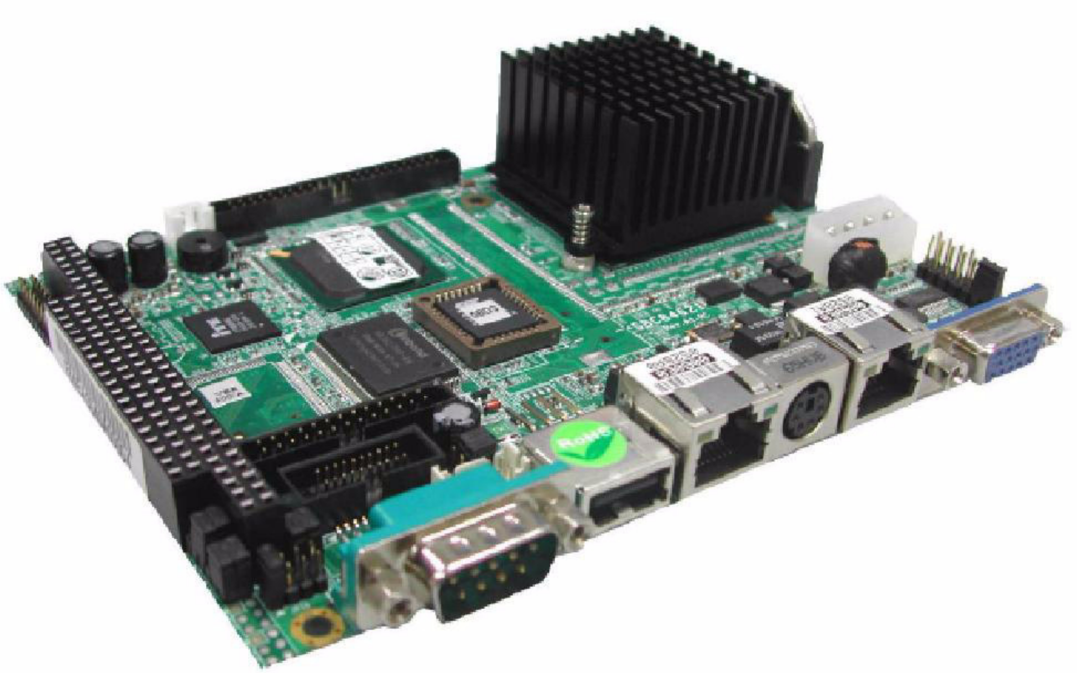


Figure 4.1 CPU Board

Specification for CPU	
Input Voltage	+5 VDC (4.75 VDC to 5.25 VDC)
Current Consumption	1.95 A @ 5 VDC
CPU speed	500 MHz
RAM	512 MB

4.1 Component Layout of the CPU Board

The following layout diagrams shows the major physical components on the CPU board. A brief description is provided on some of the major components.

There are three different types of CPU boards, hence the layout of each type will be slightly different. The diagrams below shows each type and the location of the relevant components.

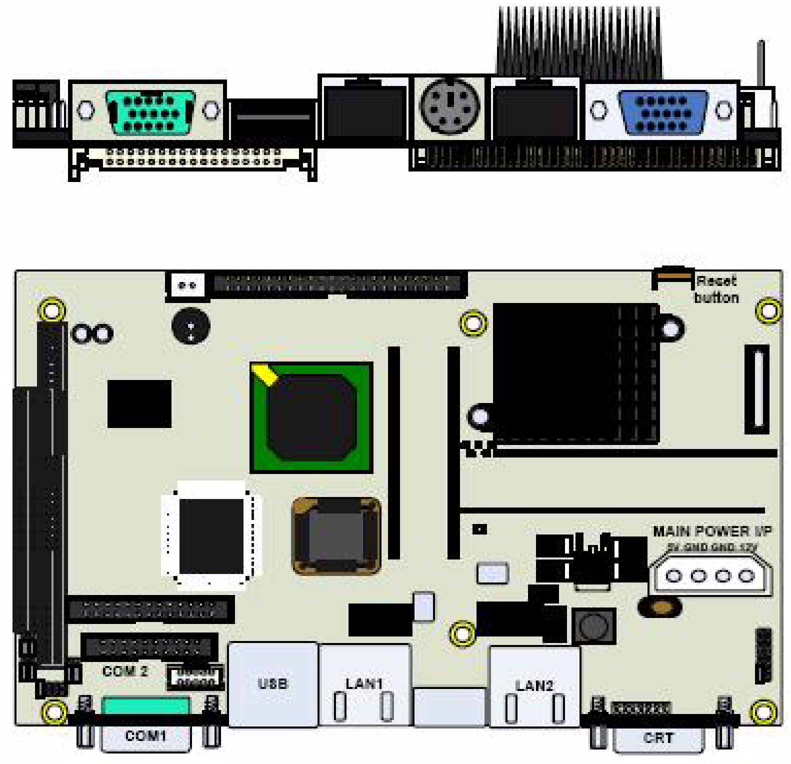


Figure 4.2 Type1 CPU Board

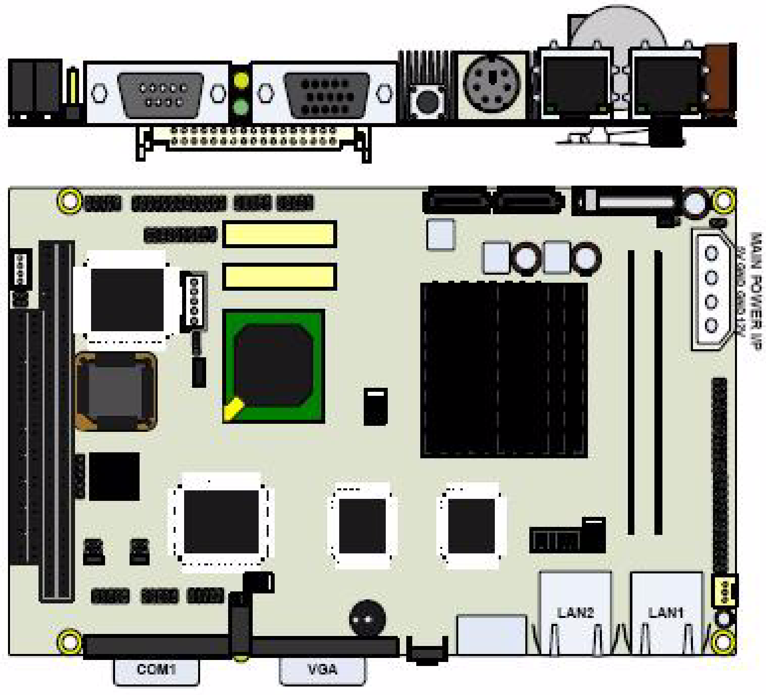


Figure 4.3 Type2 CPU Board

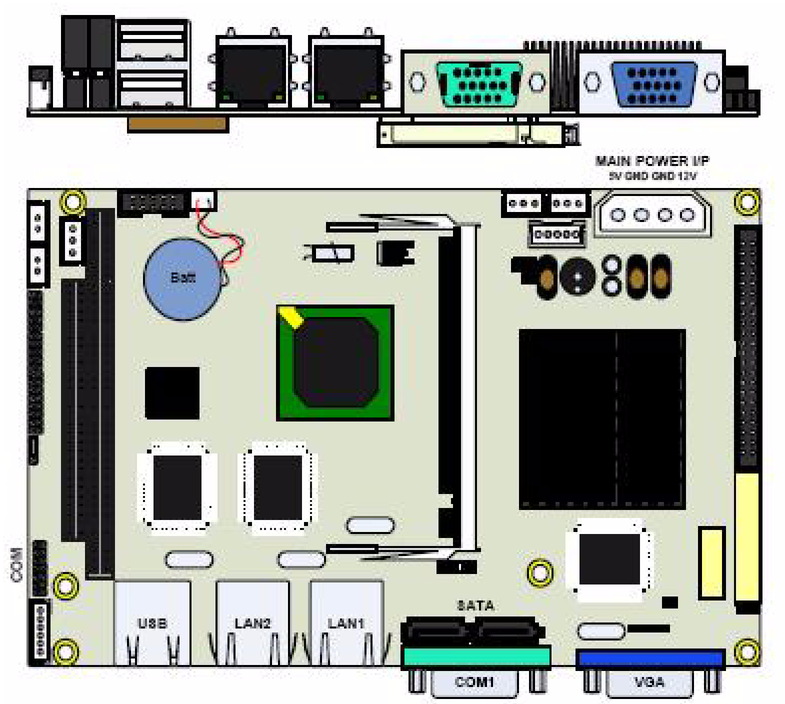


Figure 4.4 Type3 CPU Board

Ethernet Connector

A Category 5 cable is connected from this RJ45 socket to the plug-in 100BaseT Ethernet card located in the Central Monitoring Computer directly or via a hub. The table below shows the pin configuration for the socket.

100Base-Tx Ethernet connector			
1	Tx+	2	Tx-
3	Rx+	4	NC
5	NC	6	Rx-
7	NC	8	NC

Serial Port for Modem

This is a standard RS232 communication port used for modem connection. Refer to cable connection for more details.

Serial Port for the interface board

This is a 9 pins serial port. The serial port is connected to the interface boards.

RS232 Serial Port			
Pin	**Signal**	**Pin**	**Signal**
1	DCDB	2	RXDB
3	TXDB	4	DTRB
5	GND	6	DSRB
7	RTSB	8	CTSB
9	RIB	10	-

5 VDC & 12 VDC Power Input

The CPU board can be powered up by the 100~240 VAC input PSU.

Refer to Section 7 Power Supply Unit for further information before connecting any power source to the CPU board.

Power Connector	
Pin	**Signal**
1	+5V
2	GND
3	GND
4	+12Vcc

4.1.1 Other Components

Lithium Battery Holder

This is the location where a 3V Lithium battery is situated. The Lithium battery provides continuous power supply to the Real Time Clock circuitry in case of a power outage. The power will only be drawn from this battery under the following conditions: -

- No power is supplied from the PSU, and
- The external 12V rechargeable battery is not charged sufficiently, or is drained for prolong period of time and unable to provide backup power.

NOTICE!

It is recommended that this battery be changed every 2 years. Recommended replacements are the Panasonic Model CR2032 Lithium Battery for Axiom and A-Value CPU boards, or the Varta Model CR2032 Lithium Battery.

CAUTION!

Batteries should only be replaced by a qualified service technician.

5 4-Reader Board

This chapter describes one of the interface boards used by the AEC2.1 system. This section identifies and locates key components on the board and includes a brief overview of the functional operation.

The first is the 4-Reader board, which provides all the termination points needed to fully manage four card readers and all associated supporting hardware. The board size and location of mounting holes on both the 4-Reader board and 8-IO board are the same.

5.1 Technical Overview of 4-Reader Board

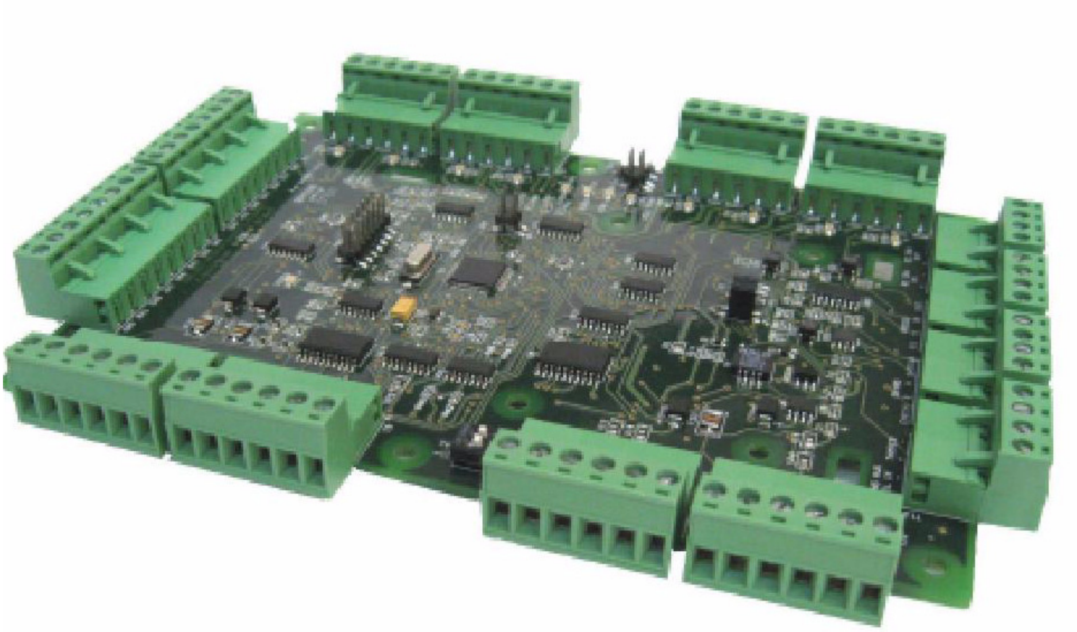


Figure 5.1 4-Reader Board

5.1.1 Component Layout of 4-Reader Board

The diagram below shows the layout and major components of the 4-Reader board. A brief technical description of the components is provided in the following pages.

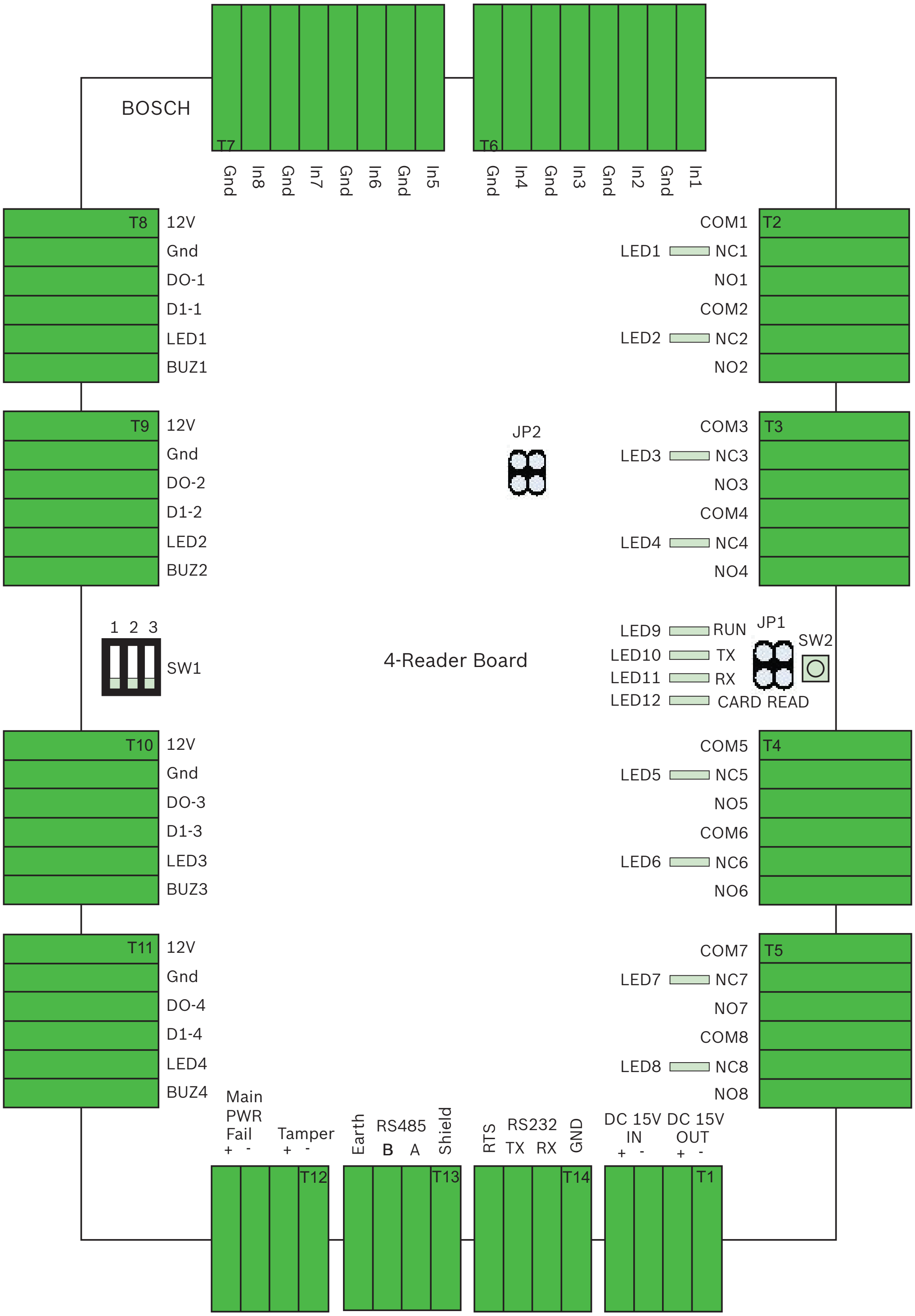


Figure 5.2 4-Reader Board Layout

5.1.2 Reader Connectors

The Reader board contains four 6-pin terminal strips down the left side of the board. Each terminal strip provides wiring terminations for one standard Wiegand output reader. The terminal strips are labelled on the board as T8, T9, T10 and T11. T8 provides the termination points for reader 1, T9 for reader 2, T10 for reader 3, and T11 for reader 4.

The pin configured for each reader connector is shown in the table below.

Pin#	Function
1	12 VDC
2	Ground
3	Data 0
4	Data 1
5	Green LED Control
6	Buzz Control

NOTICE!
Each connector is able to provide a maximum current of 150mA at 12 VDC. This is sufficient power for most readers. Readers requiring higher current will need to have the power supplied from an external power supply.

5.1.3 Input Connectors

Two 8-pin terminal strips across the top of the 4-Reader board provide termination points for the door contacts and request-to-exit devices associated with the readers. The terminal strips are identified as T6 and T7 on the 4-Reader board.

For each of the four readers this board can control, there are two terminals each for connection of a door contact and a request-to-exit device. Both circuits (contact and REX) are supervised and should be terminated according to the type of supervision applied to that particular input (*Section 9.5.1 Wiring Diagram for Supervised Inputs, page 51*). If either contact or REX device are not to be used, then the termination resistor should be installed across the terminals within the controller. Refer to *Section 9 How to Install Reader and Field Devices, page 41*, for detailed wiring diagrams.

The tables below show the various termination points on the terminal strips.

T6 Terminal Strip	
IN1	Request-to-exit for reader #1
GND	Request-to-exit for reader #1
IN2	Door contact for reader #1
GND	Door contact for reader #1
IN3	Request-to-exit for reader #2
GND	Request-to-exit for reader #2
IN4	Door contact for reader #2
GND	Door contact for reader #2

T7 Terminal Strip	
IN5	Request-to-exit for reader #3
GND	Request-to-exit for reader #3
IN6	Door contact for reader #3
GND	Door contact for reader #3
IN7	Request-to-exit for reader #4
GND	Request-to-exit for reader #4

T7 Terminal Strip	
IN8	Door contact for reader #4
GND	Door contact for reader #4

5.1.4 Output Connectors

Four 6-pin terminal strips provide connections for door strike and/or magnetic lock control. The four terminal strips are labelled on the circuit boards as T2, T3, T4 and T5. The output terminals are Form-C type dry contacts from relays located on the 4-Reader board. Each output relay provides Normally Closed (N/C), Normally Open (N/O) and a Common terminal (COM). Each relay also has a corresponding LED, that lights up whenever the relay is activated.

T2 provides output connection points for readers 1 and 2. T3 provides output connection points for readers 3 and 4. T4 provides connection points for two spare relays. T5 provides two spare relay outputs, except on the first 4-Reader board. T5, relay 8 provides a common alarm output for all Reader boards.

On the first 4-Reader board, the last relay is assigned in the software to provide a common alarm output from the controller. This relay is intended to provide an easy hand-off by the controller of an alarm indication to an external burglar alarm system. The common alarm relay will activate whenever a Door Forced Open or Door Held Open alarm is detected by the controller. It will also activate when the controller's door tamper circuit is activated, or in occurrence of an AC power failure.

The common alarm relay will reset when all alarm conditions have returned to normal. Detailed information concerning the common alarm output is provided in this manual.

NOTICE!

The contacts of all relays are rated at DC 24V/1A maximum.

The pin configuration for each output connectors is shown in the tables below.

T2 Terminal Strip (top terminal)	
Pin#	**Function**
1	Reader #1 (common)
2	Reader #1 (Normally closed)
3	Reader #1 (normally open)
4	Reader #2 (common)
5	Reader #2 (normally closed)
6	Reader #2 (normally open)

T3 Terminal Strip (second terminal from top)	
Pin#	**Function**
1	Reader #3 (common)
2	Reader #3 (Normally closed)
3	Reader #3 (normally open)
4	Reader #4 (common)

T3 Terminal Strip (second terminal from top)	
Pin#	**Function**
5	Reader #4 (normally closed)
6	Reader #4 (normally open)

T4 Terminal Strip (third terminal from top)	
Pin#	**Function**
1	Spare (common)
2	Spare (Normally closed)
3	Spare (normally open)
4	Spare (common)
5	Spare (normally closed)
6	Spare (normally open)

T5 Terminal Strip (bottom terminal)	
Pin#	**Function**
1	Spare (common)
2	Spare (Normally closed)
3	Spare (normally open)
4	Common Alarm Output (common)
5	Common Alarm Output (normally closed)
6	Common Alarm Output (normally open)

NOTICE!

The common alarm output relay only exists on the first 4-Reader board. On boards 2, 3 and 4 this relay is an additional spare.

5.1.5 15 VDC Input Termination

Reference: Terminal Strip T1

Terminal strip T1 is used to provide up to 15 VDC power to the interface boards (e.g. 4-Reader board and 8-IO board). It consists of four terminals. Two terminals provide the input power for the board (DC 15V IN), and the next two terminals provide the input power for the next board (DC 15V OUT), within the same casing. The diagram below shows the configuration of the terminal strip T1. It receives 13 VDC from the PSU.

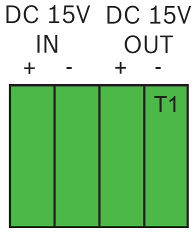


Figure 5.3 15 VDC Input Terminal

5.1.6 RS232

Reference: Terminal Strip T14

Terminal strip T14 is used as a communication channel between the interface board (e.g. 4-Reader board and 8-IO board) and the CPU. The channel consists of four data cables, namely RTS, TX, RX, and Gnd. The cables are connected to the serial COM port on the CPU. The diagram below shows the configuration of the terminal strip T14.

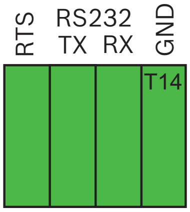


Figure 5.4 RS232

5.1.7 RS485

Reference: Terminal Strip T13

Terminal strip T13 is used as a communication channel between the interface boards (e.g. 4-Reader board and 8-IO board). RS485 is a multi-drop communication channel. It enables the CPU to disseminate and receive data to and from all the interface boards. It consists of four 24-AWG-CAT5 cables, namely EARTH, B, A and SHIELD. All the interface boards within the system are connected using the RS485 terminal. The diagram below shows the connections on the terminal strip T13.

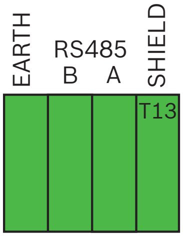


Figure 5.5 RS485

5.1.8 Tamper and Main Power Fail

Reference: Terminal Strip T12

Terminal strip T12 comprises of Tamper alarm and Main Power Fail alarm inputs. The Tamper terminals are connected to a micro-switch that is used to monitor the enclosure's cover against unauthorized tampering. Any opening of the enclosure cover will trigger the Common Alarm output and sounds off the CPU buzzer. A Controller Tamper alarm message is sent to the Transactions page of the AEC2.1 user software.

The Main Power Fail alarm will be triggered when the input AC power is cut off and the backup battery takes over. The terminals will be shorted together.

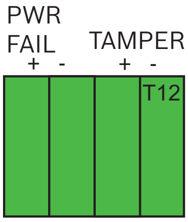


Figure 5.6 Tamper and Main Power Fail

5.1.9 LED Indicators

Reference: LED 1 to LED 8

LEDs 1 to 8 light whenever the associated relay is activated.

Reference: LED9

This LED indicates that the processor on the 4-Reader board is running.

Reference: LED 10 and LED 11

These LEDs should blink in normal operation. This indicates normal communication between the 4-Reader board and the CPU board.

Reference: LED 12

This LED will blink once each time card is presented to a reader.

5.1.10 Reset Button

Reference: SW2

SW2 is a reset button to reset the processor on the interface board.

5.1.11 End-of-Line Setting

Reference: JP1

AEC2.1 uses RS485 multi-drop communication channels between the CPU and interface boards. It is necessary to include the end-of-line jumper settings on the last interface board in configuration to have a stable communication channel.

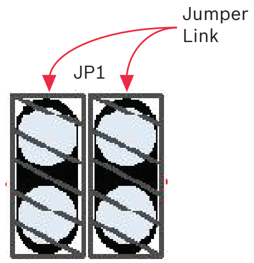
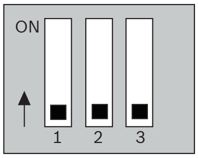
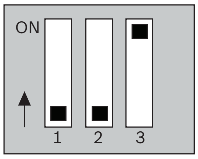
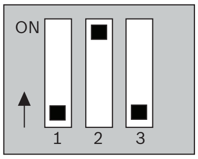
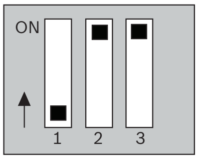


Figure 5.7 Jumper Setting

5.1.12 Address Setting Switch

Reference: SW1

SW1 is switch to set the address of individual interface boards. It consists of two dip switches for setting of the address in binary sequence. Each AEC2.1 can manage up to eight 4-Reader boards and eight 8-IO boards. The address settings for the 4-Reader boards are shown in the table below.

Address setting using SW1 for the 1st and 5th 4-Reader board in AEC2.1 system.		The 1st 4-Reader board will consist of readers 1 to 4 The 5th 4-Reader board will consist of readers 17 to 20
Address setting using SW1 for the 2nd and 6th 4-Reader board in AEC2.1 system.		The 2nd 4-Reader board will consist of readers 5 to 8 The 6th 4-Reader board will consist of readers 21 to 24
Address setting using SW1 for the 3rd and 7th 4-Reader board in AEC2.1 system.		The 3rd 4-Reader board will consist of readers 9 to 12 The 7th 4-Reader board will consist of readers 25 to 28
Address setting using SW1 for the 4th and 8th 4-Reader board in AEC2.1 system.		The 4th 4-Reader board will consist of readers 13 to 16 The 8th 4-Reader board will consist of readers 29 to 32

NOTICE!
The boards are addressed in binary sequence. AEC2.1 can support up to 16 interface boards, eight 4-Reader boards and eight 8-IO boards. The address pin ‘1’ is reserved for future development, to expand the capability of AEC2.1.

5.1.13 Factory Default Setting

Reference: JP2
JP2 of the first 4-Reader board is used to reset the AEC2.1 back to factory default. JP2 carries two functions:

- Clearing all information, settings and configuration. (IP address will not be reset with this function)
- Resetting the IP address of the panel back to default IP

Refer to *Section 24 Appendix H Resetting to Factory Default, page 118* for detail instructions.

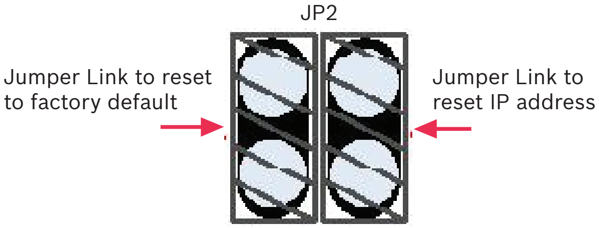

JP2
Jumper Link to reset to factory default
Jumper Link to reset IP address

Figure 5.8 Factory Default Setting

CAUTION!

- Resetting the system to factory default settings will clear the data stored in the AEC2.1 system. Be sure to do a backup of the system before resetting.
- After rebooting the system, remove the jumper links from the 4-Reader board.
- This function is only available to the first 4-Reader board of the AEC2.1 configuration, although all the 4-Reader board comes with JP2.

6 8-Input-Output Board

This chapter describes one of the interface boards employed by the AEC2.1. This section identifies and locates key components on the board and includes a brief overview of the functional operation.

The 8-IO board provides eight zones of end-of-line resistor type inputs and eight contact closure outputs. This board is intended for non-reader type applications where it is desirable to monitor emergency exit doors, or motion detectors. This board also provides eight Form-C type relay outputs, which can be used to control external equipment, such as lights, gate motor, etc.

The board size and location of mounting holes on both the 4-Reader board and 8-IO board are the same.

6.1 Technical Overview of 8-Input-Output Board

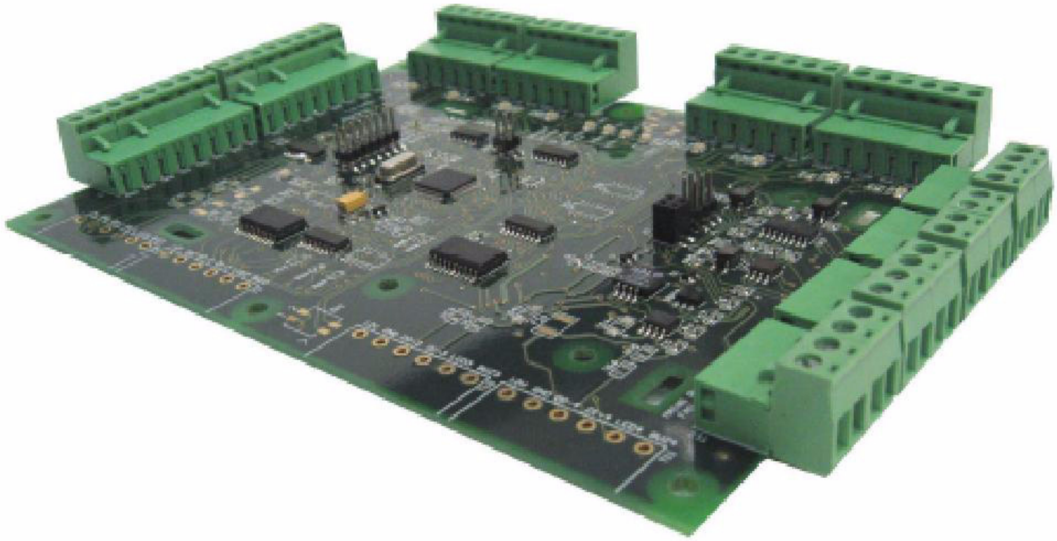


Figure 6.1 8-Input-Output Board

6.1.1 Component Layout of 8-Input-Output Board

The diagram below shows the layout of 8-IO board. All major components are identified on the diagram, and a brief technical description is provided in the following pages.

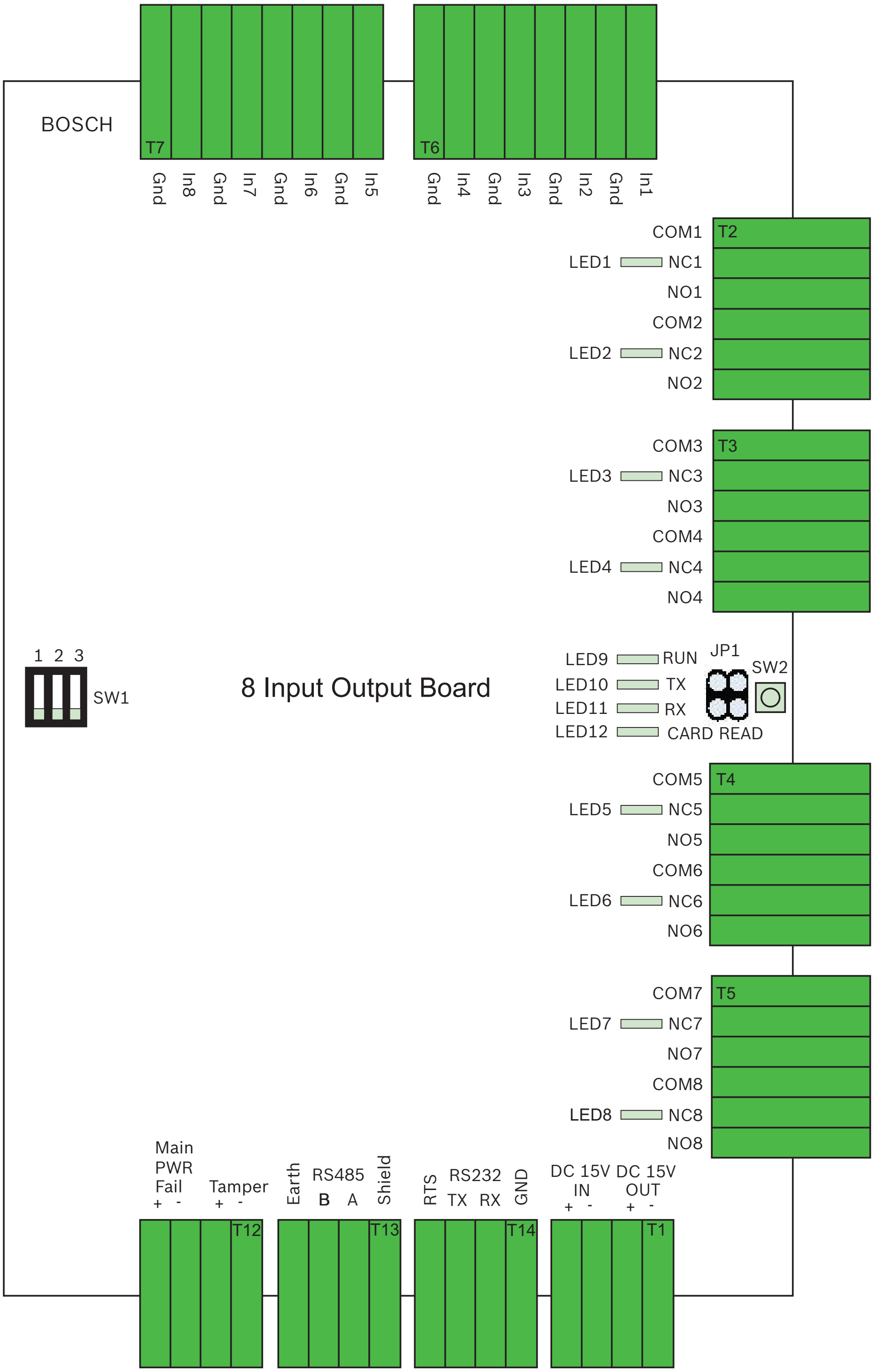


Figure 6.2 Layout of 8-Input-Output Board

6.1.2 Input Connectors

Two 8-pin terminal strips across the top of the 8-IO board provide termination points for wiring from door contacts and other alarm sensors. The terminal strips are identified as T6 and T7 on the 8-IO board.

There are two terminals for each input point. Each input point is supervised and must be terminated according to the type of supervision applied to that particular input (Refer to *Section 9.5.1 Wiring Diagram for Supervised Inputs, page 51*). All unused points should have the termination resistor installed across the terminals within the controller. Refer to *Section 5 4-Reader Board, page 19* for detailed wiring diagrams.

The charts below show the various termination points on the terminal strips.

T6 Terminal Strip	
IN1	Input Point #1
GND	Input Point #1
IN2	Input Point #2
GND	Input Point #2
IN3	Input Point #3
GND	Input Point #3
IN4	Input Point #4
GND	Input Point #4

T7 Terminal Strip	
IN5	Input Point #5
GND	Input Point #5
IN6	Input Point #6
GND	Input Point #6
IN7	Input Point #7
GND	Input Point #7
IN8	Input Point #8
GND	Input Point #8

6.1.3 Output Connectors

Four 6-pin terminal strips provide connection points for connection of external devices controlled by the AEC2.1. The terminal strips are labelled on the circuit board as T2, T3, T4 and T5. The output terminals are Form-C type dry contacts from relays located on the 8-IO board. For each relay, Normally Closed (N/C), Normally Open (N/O) and a Common terminal (COM) are provided.

NOTICE!

The contacts of all relays are rated at DC 24V/1A maximum

The relay contacts can be connected directly to many low voltages DC powered devices, including alarm bells, security lights, horns, etc. When using the outputs to control high voltage devices, such as lighting circuits, electric door controllers, gate motors, etc., an external interface relay must always be used. Also, use an external relay when interfacing with AC-power devices.

In all instances where the output relay is used to operate an inductive load, such as when interfacing with an external relay, or powering the coil of an alarm bell, a back-biased diode should be wired across the coil of the driven device. This will protect the electronic circuitry on the 8-IO board by providing suppression from back-emf when the devices are deactivated.

Each output relay on the 8-IO board also has a corresponding LED which lights up whenever the relay is activated.

Beginning from the top of the 8-IO board, T2 provides connection points for outputs 1 and 2. T3 provides connection points for outputs 3 and 4. T4 provides connection points for outputs 5 and 6. T5 provides connection points for outputs 7 and 8. The pin configuration for each output connector is shown in the tables below.

T2 Terminal Strip (top connector)	
Pin#	**Function**
1	Output #1 (common)
2	Output #1 (normally closed)
3	Output #1 (normally open)
4	Output #2 (common)
5	Output #2 (normally closed)
6	Output #2 (normally open)

T3 Terminal Strip (second connector from top)	
Pin#	**Function**
1	Output #3 (common)
2	Output #3 (normally closed)
3	Output #3 (normally open)
4	Output #4 (common)
5	Output #4 (normally closed)
6	Output #4 (normally open)

T4 Terminal Strip (third connector from top)	
Pin#	**Function**
1	Output #5 (common)
2	Output #5 (normally closed)
3	Output #5 (normally open)
4	Output #6 (common)
5	Output #6 (normally closed)
6	Output #6 (normally open)

T5 Terminal Strip (bottom connector)	
Pin#	**Function**
1	Output #7 (common)
2	Output #7 (normally closed)
3	Output #7 (normally open)
4	Output #8 (common)

T5 Terminal Strip (bottom connector)	
Pin#	**Function**
5	Output #8 (normally closed)
6	Output #8 (normally open)

6.1.4 15 VDC Input Termination

Reference: Terminal Strip T1

Terminal strip T1 is used to provide a 15 VDC power to the interface boards (e.g. 4-Reader board and 8-IO board). It consists of four terminals: two of which are for the input power for the board (DC 15V IN), and the next two provide the input power for the next board (DC 15V OUT), within the same casing. The diagram below shows the configuration of the terminal strip T1.

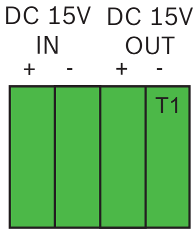


Figure 6.3 Input Terminal

6.1.5 RS232

Reference: Terminal Strip T14

Terminal strip T14 is used as a communication channel between the interface board (e.g. 4-Reader board and 8-IO board) and the CPU. The channel consists of four data cables, namely RTS, TX, RX, and Gnd. The cables are connected to the serial COM port on the CPU. The diagram below shows the configuration of the terminal strip T14.

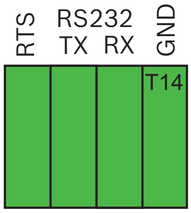


Figure 6.4 RS232

6.1.6 RS485

Reference: Terminal Strip T13

Terminal strip T13 is used as a communication channel between the interface board (e.g. 4-Reader board and 8-IO board) and the CPU. RS485 is a multi-drop communication channel. It enables the CPU to disseminate and receive data to and from all the interface boards. It consists of four 24-AWG-CAT5 cables, namely EARTH, B, A and SHIELD. All the interface boards within the system are connected using the RS485 terminal. The diagram below shows the connection on the terminal strip T13.

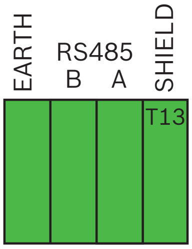


Figure 6.5 RS485

6.1.7 Tamper and Main Power Fail

Reference: Terminal Strip T12
Terminal strip T12 comprises of Tamper alarm and Main Power Fail alarm inputs. The Tamper terminals are connected to a micro-switch that is used to monitor the enclosure's cover against unauthorized tampering. Any opening of the enclosure cover will trigger the Common Alarm output and sounds off the CPU buzzer. A Controller Tamper alarm message is sent to the Transactions page of the AEC2.1 user software.

The Main Power Fail alarm will be triggered when the input AC power is cut off and the backup battery takes over. The terminals will be shorted together.

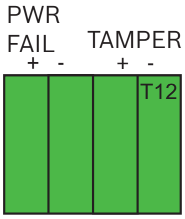


Figure 6.6 Tamper and Main Power Fail

6.1.8 LED Indicators

Reference: LED 1 to LED 8
LEDs 1 to 8 light whenever the associated relay is activated.

Reference: LED9
This LED indicates that the processor on the 8-IO board is running.

Reference: LED 10 and LED 11
These LEDs should blink in normal operation. This indicates normal communication between the 8-IO board and the CPU board.

This LED is not used by the 8-IO board.
This LED is not used by the 8-IO board.

6.1.9 Reset Button

Reference: SW2
SW2 is a reset button to reset the processor on the interface board.

6.1.10 End-of-Line Setting

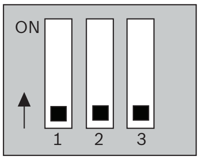
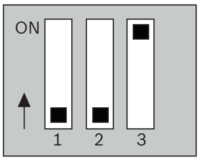
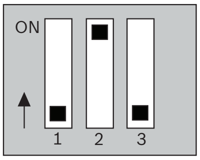
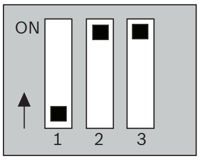
Reference: JP1

AEC2.1 uses RS485 multi-drop communication channels between the CPU and the interface boards. It is necessary to include the end-of-line jumper settings on the last interface board in configuration to have a stable communication channel.

6.1.11 Address Setting Switch

Reference: SW1

SW1 is switch for user to set the address of individual interface boards. It consist of three dip switches for setting of the address in binary sequence. Each AEC2.1 can manage up to eight 4-Reader boards and eight 8-IO boards. The address settings for the 8-IO boards are shown in the table below.

Address setting using SW1 for the 1st and 5th 8-IO board in AEC2.1 system.	
Address setting using SW1 for the 2nd and 6th 8-IO board in AEC2.1 system.	
Address setting using SW1 for the 3rdand 7th 8-IO board in AEC2.1 system.	
Address setting using SW1 for the 4th and 8th 8-IO board in AEC2.1 system.	

NOTICE!

The boards are addressed in binary sequence. AEC2.1 can support up to 16 interface boards, eight 4-Reader and eight 8-IO boards. The address pin ‘1’ is reserved for future development, to expand the capability of AEC2.1.

7 Power Supply Unit

This chapter provides an overview of the Power Supply Unit (PSU) used in AEC2.1. This chapter describes the PSU terminal layout and its power specification.

The PSU used in AEC2.1 has an input voltage of 100~240 VAC. The PSU outputs voltages for charging up the backup battery, to power up the CPU board, and to power up the interface boards.

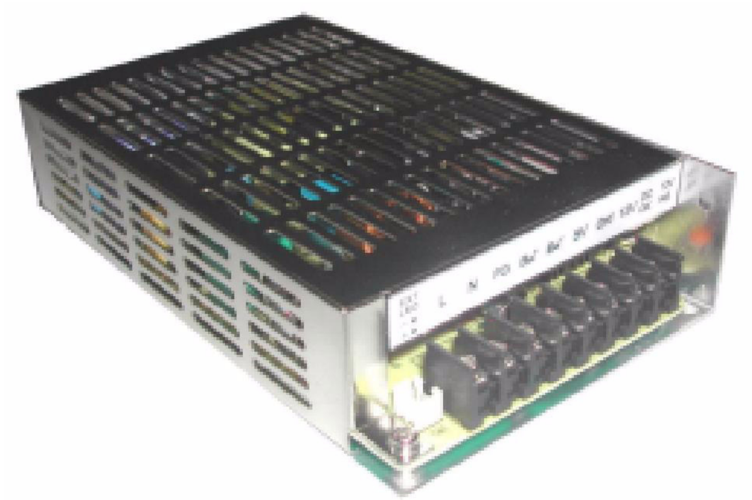


Figure 7.1 PSU with Input Voltage of 100~240 VAC

7.1 Layout of Power Supply Unit

The diagram below shows the layout of the PSU. The mechanical dimensions and technical specifications are shown in the diagram.

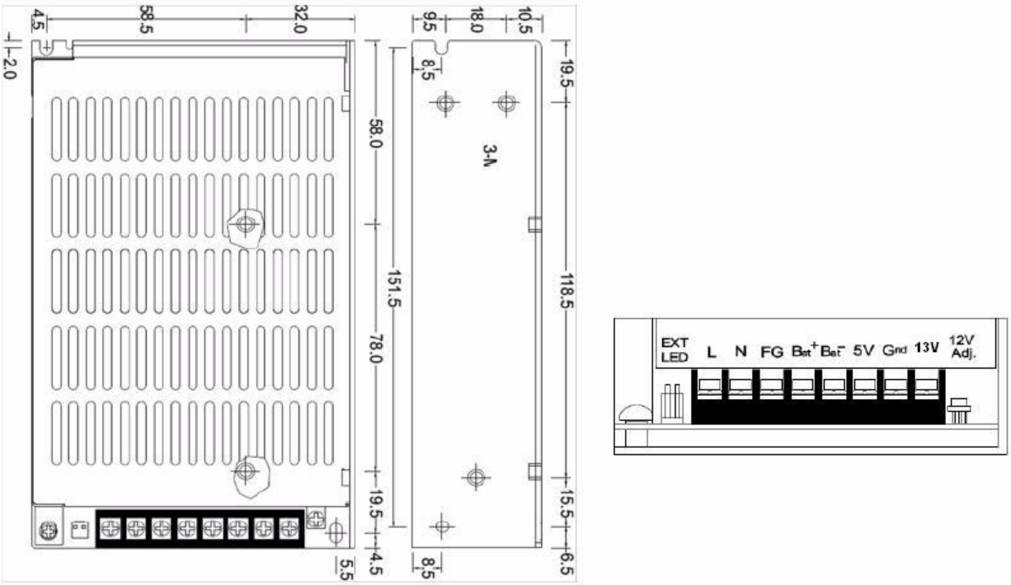


Figure 7.2 Mechanical layout of the PSU with input voltage of 100~240 VAC

WARNING!
Do not connect Live, Neutral and Ground directly onto the PSU terminals. Connect the input power cable to the power socket on the AEC2.1.

7.2 Technical Specification of Power Supply Unit with Input Power of 100~240 VAC

The table below shows the technical specifications of the PSU (input power of 100~240 VAC)

Input Voltage	100 ~ 240 VAC; 50/60 Hz
Input Voltage - UL	110 VAC; 60 Hz
Input Current	1.5A
Environment Temperature	0 - 50 degree C
Environment Humidity	non condensing 5% ~ 85% +/-5% RH
Output Current @ 13 VDC (Min./ Rated/ Max)	0/ 2.5 A/ 3.5 A
Output Current for battery charging @ Bat^+ and Bat^- (Min./ Rated/ Max)	0/ 0.23 A/ 0.23 A
Output Current @ 5 VDC (Min./ Rated/ Max)	0/ 3 A/ 4 A

7.3 Power Supply Requirement and Connection

This section describes the power supply requirement for all the electronics within each AEC2.1 enclosure and its connection.

The PSU in AEC2.1 will consume a 100~240 VAC input power. In order to provide uninterrupted power source to the system during a supply outage, a battery charging circuit is incorporated to charge the backup rechargeable battery. A 7Ah battery is needed for a 4 hour standby as required by UL294. When input power is present, the backup battery is trickle charged.

WARNING!
There is a danger of explosion if the battery is incorrectly replaced. Replace only with the same type recommended. Refer to *Section 20 Appendix D Selecting A Correct Battery Size, page 100* for information on backup battery.

7.4 Current Consumption

The table below shows the current consumption of the various types of boards.

Description	**Average Current consumption (DC)**
CPU board	1.35 A @ 5 VDC
4-Reader board	280 mA @ 12 VDC
8-IO board	280 mA @ 12 VDC

The indicated value for 4-Reader board and 8-IO board is the total current consumption of all activated relays.

The data in the table are meant to be use as a general guide. It is the responsibility of the system installer to determine the actual current consumption of the hardware that the external battery is to support in order to provide continuous supply for a known period.

TIP: If a longer Backup time is desired, it is recommended that all the Readers take its supply from another external PSU with its own back-up battery.

For system that could not be contained within the Main Enclosure, such as a 10-Door AEC2.1, additional Extension unit is added. In such case, the supply to the cards in the Extension unit(s) are provided via its own PSU in the enclosure.

NOTICE!
The table only takes into consideration the current consumption of the CPU, 4-Reader boards and 8-IO boards and does not include current consumption of the locks and the readers for each door. In practice, a separate power supply is used to provide supplies to Locks.

7.5 Connection in the Main Controller

The Main Controller is powered by the 100~240 VAC Input PSU. The 13.6 +/- 0.1 VDC output from the PSU is designed to supply power to all relays in all the interface boards, within the Main Controller Enclosure. However, when additional interface boards are installed in Extension unit/s, separate PSU must be installed, and the current ratings of these power supplies must be computed to be adequate

8 Access Easy Extension Unit

The interface boards accept 13.6 +/- 0.1 VDC from the PSU. This is used in add-on Extension unit. The PSU provides power supply to all the relays on the Interface boards.

The diagram below shows the connection between AEC2.1 main controller unit and the Extension unit.

NOTICE!

- The diagram below is for example only. Note that 8-IO board is connected up in a similar manner as shown below, through a RS485 channel.
- The Earth terminals of each boards are connected to the panel’s enclosure.

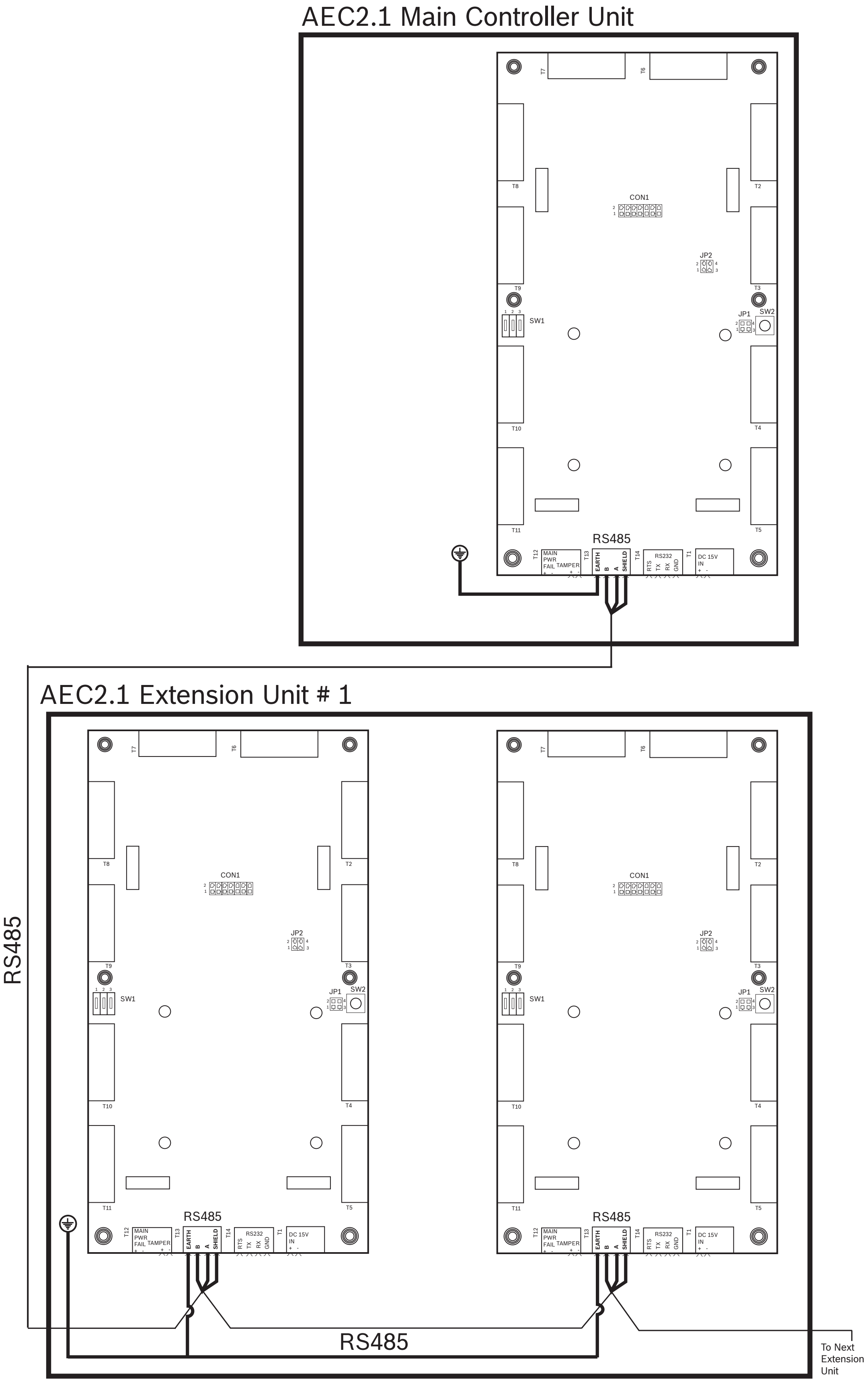


Figure 8.1 Connection between the AEC2.1 Main Controller Unit and Extension Units via RS485 communication channel.

8.1 Upgrading AEC2.1 to Support Additional Four 4-Reader Boards and Four 8-IO Boards

Using a **LAN Converter**, AEC2.1 system can be extended to support additional four 4-Reader boards and four 8-IO boards. The converter UDS1100 can be linked to AEC2.1’s CPU LAN port through an Ethernet network port to provide an additional multidrop communication channel. This UDS 1100 can be mounted over the reader board (Refer to quick start guide for UDS 1100).

After mounting the device over the reader board, it needs to be connected to the CPU LAN port of AEC2.1 through LAN (Ethernet) cable. There is a serial port RS485 from the device which is connected to the main power and the reader board.

Figure 8.2 shows the wiring picture for the connections.

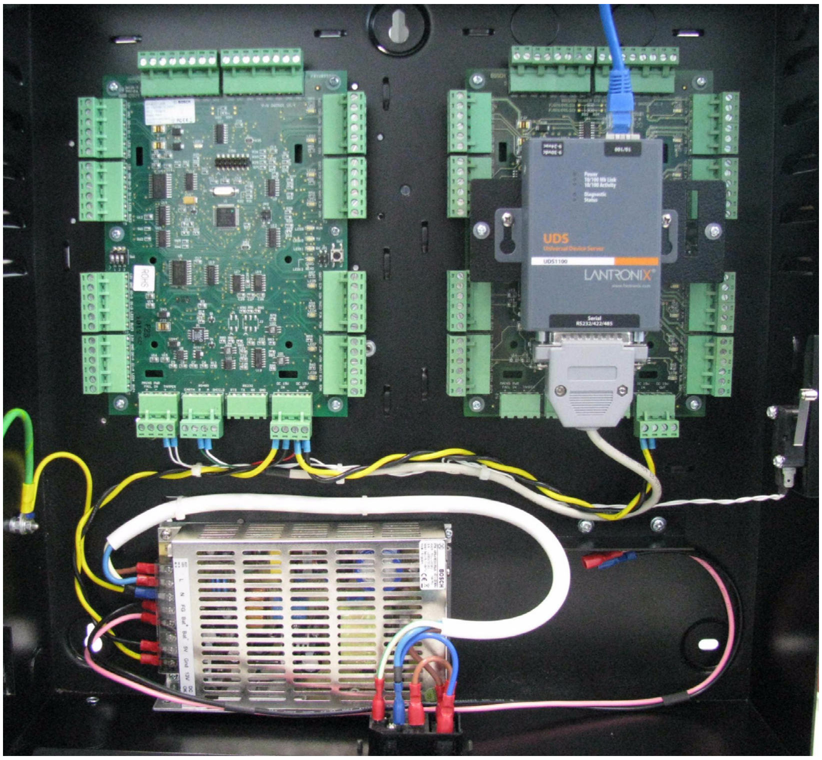


Figure 8.2 Reader board with UDS1100

Alternatively UDS1100 can also be placed next to the reader board and connected (refer to quick start guide for UDS 1100). The UDS 1100 is pre-configured with default **IP address** and **Subnet Mask**. The user can connect it to the CPU, and access the extension panel by keying in the default IP address in the web browser. (Refer to quick start guide for UDS 1100 for details).

Disclaimer: Lantronix module is not been investigated by UL.

9 How to Install Reader and Field Devices

This section summarizes the installation requirements for readers, door strikes and magnetic locks, door contacts, request-to-exit devices, and miscellaneous alarm devices.

- HID MiniProx Reader
- HID ProxPro with Keypad Reader
- HID ProxPro without Keypad Reader
- HID ProxPoint Reader

Before mounting or wiring any hardware, be sure to read and understand the manufacturer's documentation provided with each piece of equipment.

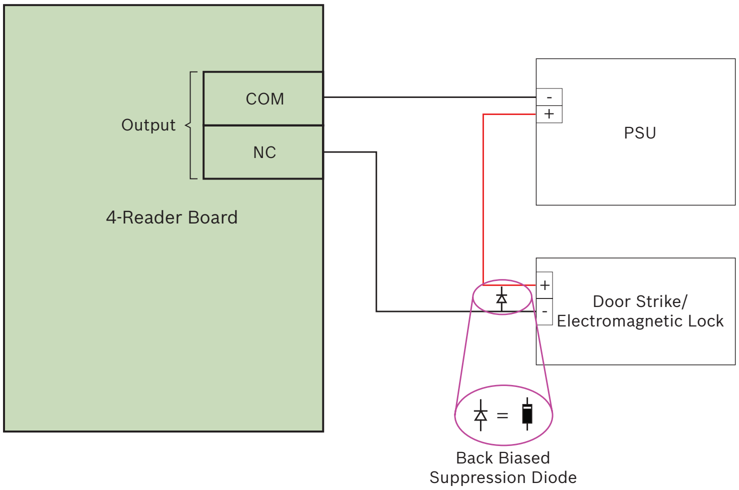
Also, be sure to use wire types and installation practices in full compliance with all applicable codes, and in conformance with all requirements of local jurisdictional authorities.

1. Mount and wire readers in accordance with the manufacturer's instructions provided with the readers.
   - When mounting a reader on a metal mullion or metal junction box, the screws provided with the reader must be used. When mounting the reader on any other surface, use appropriate fasteners.
   - The shield drain wire from the reader cable should be spliced to the shield conductor of the reader cable coming from AEC2.1. The cables shield must be left floating at the controller end. This configuration provides the best shielding from external interference, and minimizes the likelihood of reader generated interference.

2. Mount and wire door strikes and/or electric locks.
   - Wire in accordance with manufacturer's instructions.
   - The door strike relays on the 4-Reader boards are designed to handle 1A@ 24 VDC Resistive. This should satisfy most door strikes and magnetic locks. Should larger current locks or strikes need to be controlled, then external interface relays must be installed. External interface relay should also be used with all AC-powered door strikes.

VERY IMPORTANT: A suppression diode must be installed across the coil of all DC powered door strikes and magnetic locks. The diode provides protection against the back-emf that is generated when a strike/lock coil is de-energized. Refer to the door-wiring diagram for additional details.

WARNING!
Never connect a door strike or magnetic lock circuit to AEC2.1 or any other Access Controller without installing the protection diode.



IMPORTANT: The above figure shows the connection of a back EMF diode on the door strike

3. Mount and wire door contacts and request-to-exit devices.
   - Install 6.8K ohm end-of-line resistors at each devices. The resistor should be wired in parallel (across) normally open devices and in series with normally closed devices. Refer to door wiring diagrams for additional details.
   - When using PIR type request-to-exit devices, be sure to read manufacturers instructions carefully. Many of these devices need an internal jumper position changed to work properly in access control applications. Changing this jumper setting allows the units to quickly reset after they have detected motion. Without changing the jumper, some devices take up to 30 seconds to reset after they detect motion. Refer to manufacturer's instruction for additional details.
   - Wireless PIR devices are not recommended for use in access control systems and should not be used as request-to-exit devices on AEC2.1 applications.

4. Wire any output devices that are to be controlled by the controller.
   - Output circuits are typically used to control alarm bells, lighting circuits, or similar equipment.
   - The output relays on the AEC2.1 interface boards are designed to handle 1A @ 24 VDC Resistive. If it is necessary to control larger current devices or AC powered devices, then external interface relays must be installed.

5. Connect all field devices wiring to the 4-Reader and 8-IO boards in the AEC2.1.
   - Refer to the device wiring diagrams in this manual to identify the termination points for the various devices.
   - All controller termination land on removable terminal strips. We suggest you carefully remove the terminal strips before landing the wires. Once all wires have been landed on a terminal strip and verified, gently re-insert the terminal strip on the circuit board.
   - If wiring directly to the terminal strips without first removing the strip from the board, use caution that bare wires do not accidentally touch any components or foils on the circuit boards.
   - Terminate all unused door contact and request-to-exit circuits by connecting a 6.8K ohm resistor directly across the appropriate terminals. Also terminate unused input zones on 8-IO boards.

The following pages contains door wiring diagrams for some most common HID readers used with the AEC2.1. This section provides instructions on how to test the readers.

The following readers have been verified by UL for compatibility with the controller:

- HID MiniProx Reader
- HID ProxPro with Keypad Reader
- HID ProxPro without Keypad Reader
- HID ProxPoint Reader

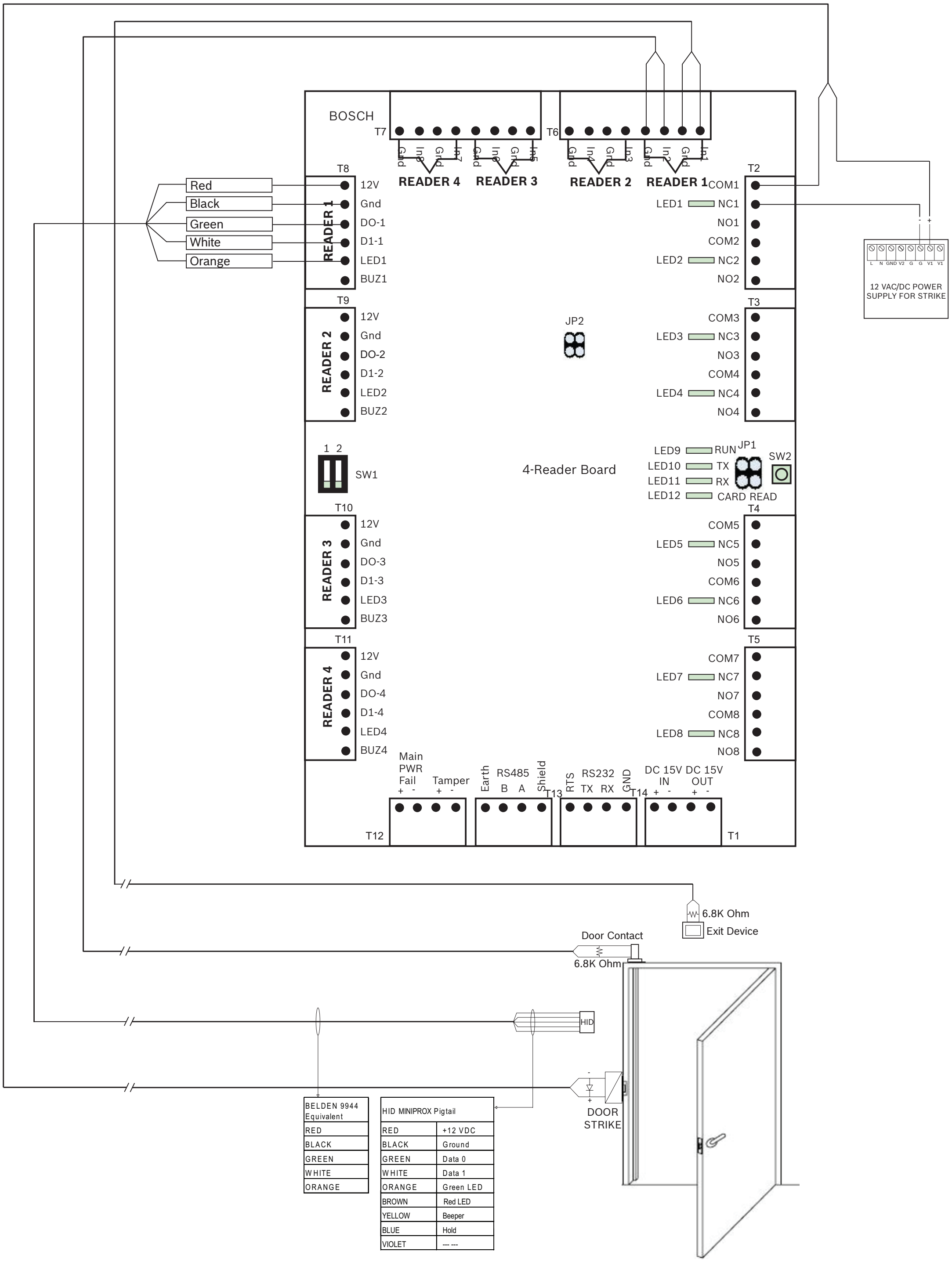
NOTICE!
Refer to *Section 11 Card Reader Keypad Functions, page 56* for a detail description on the AEC2.1 reader Keypad functions.

9.1 HID MiniProx Reader

1. Connect the terminal strip where the cable from the reader is terminated to the proper connector on the 4-Reader board.
   Result: The reader LED will alternately flash between red & green for a few seconds, and the beeper in the reader will beep three times in a sequence of two beeps, short pause, one beep. The LED will remain lit in red.

2. Present a card to the reader.
   Result: The green LED should light briefly and the reader should sound a short beep. This indicates that the reader recognized the card.

3. Depending on the setup of the controller database for the card used in the previous step, one of two events will occur within a second of the beep in step 2. Note that either response indicates that the reader is working.
   - If the card is configured to allow access through the reader, then the LED will light in green for a few seconds indicating that access has been granted.
   - Or, if the database has not yet been configured, then the LED will flash between red & green in a rapid alternating pattern for two to three seconds indicating that access has been denied.



BELDEN 9944 Equivalent
RED
BLACK
GREEN
WHITE
ORANGE

HID MINIPROX Pigtail	
RED	+12 VDC
BLACK	Ground
GREEN	Data 0
WHITE	Data 1
ORANGE	Green LED
BROWN	Red LED
YELLOW	Beeper
BLUE	Hold
VIOLET	--- ---

Note:

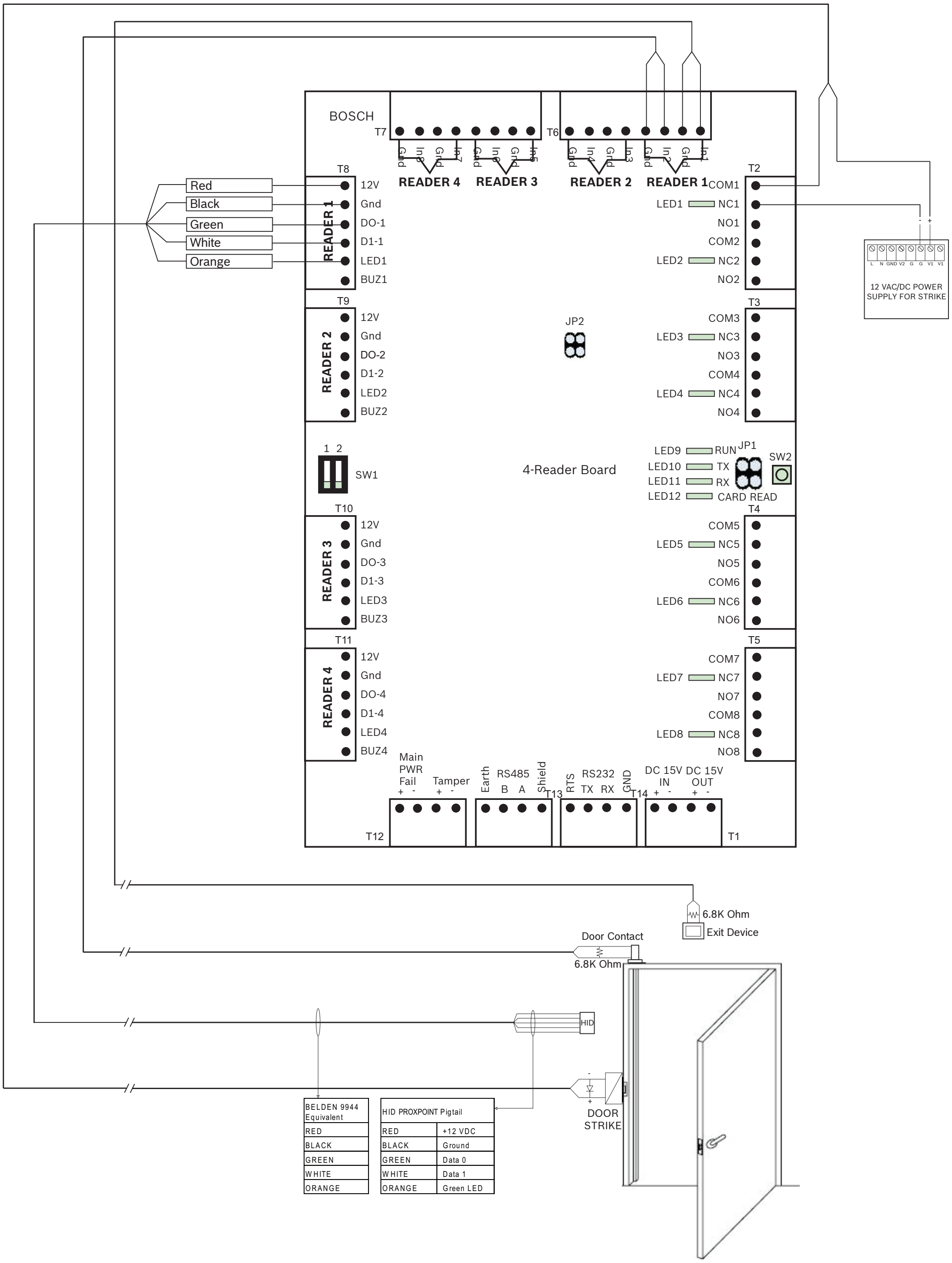
- All interconnected devices must be UL Listed
- UL listed and/or recognized wire must be used for cabling and wire suitable for the application.

9.2 HID ProxPoint Reader

1. Connect the terminal strip where the cable from the reader is terminated to the proper connector on the 4-Reader board.
   Result: The reader LED will alternately flash between red & green for a few seconds. Then the LED will remain lit in red.

2. Present a card to the reader.
   Result: The LED should light in green briefly indicating that the reader recognized the card.
   – If the card is configured to allow access through the reader, then the door strike relay on the reader board will activate and the red door strike LED on the same board will light indicating that access has been granted.

3. Depending on the setup of the controller database for the card used in the previous step, one of two events will occur within a second of the beep in step 2. Note that either response indicates that the reader is working.
   – If the card is configured to allow access through the reader, then the LED will light in green for a few seconds indicating that access has been granted.
   – Or, if the database has not yet been configured, then the LED will flash between red & green in a rapid alternating pattern for two of three seconds indicating that access has been denied.



BELDEN 9944 Equivalent
RED
BLACK
GREEN
WHITE
ORANGE

HID PROXPOINT Pigtail	
RED	+12 VDC
BLACK	Ground
GREEN	Data 0
WHITE	Data 1
ORANGE	Green LED

9.3 HID ProxPro Reader

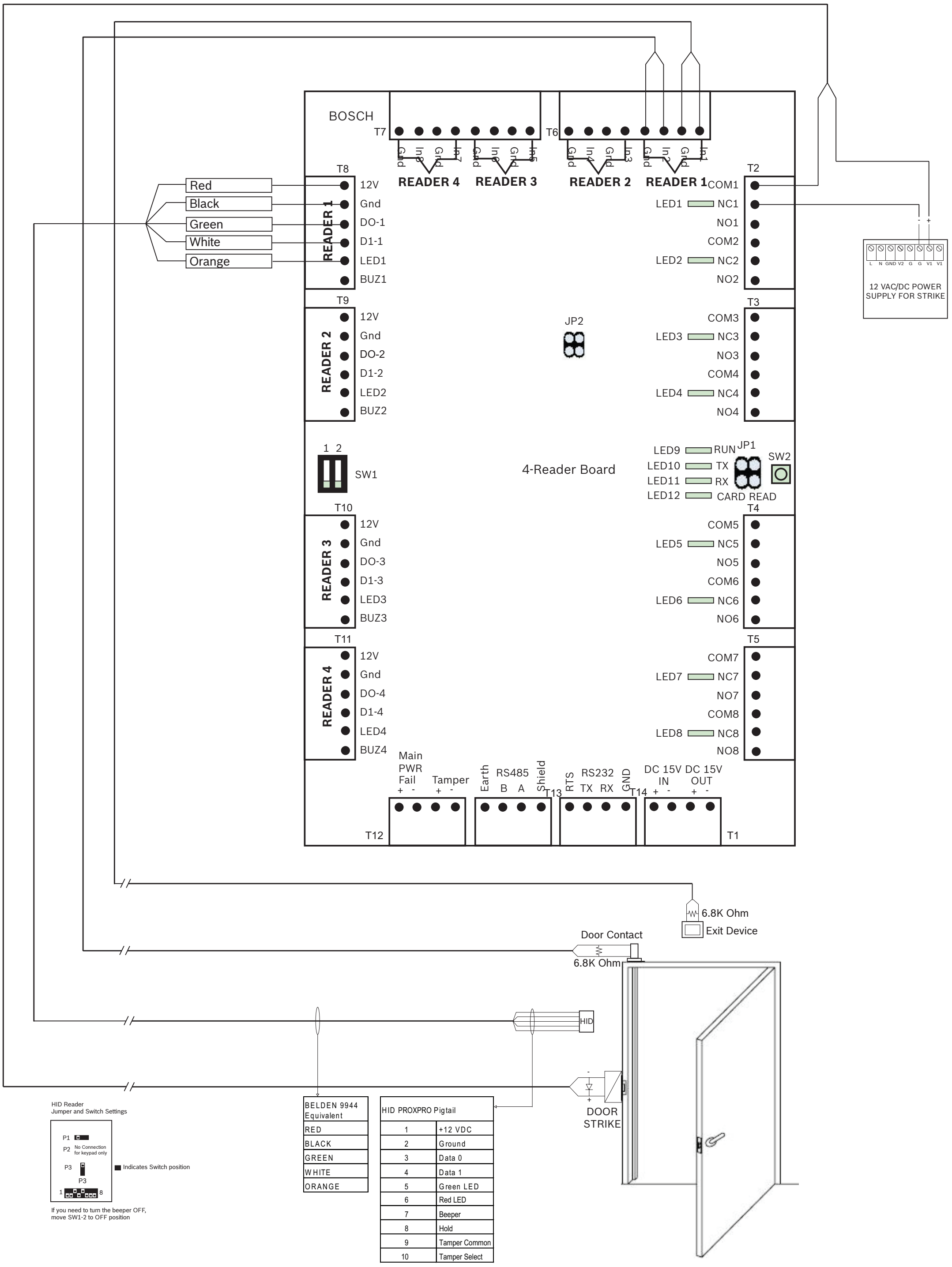
1. Connect the terminal strip where the cable from the reader is terminated to the proper connector on the 4-Reader board.
   Result: The reader LEDs will alternately flash between red & green for a few seconds, and the beeper in the reader will beep three times in a sequence of 2 beeps, short pause, one beep. The LED will remain lit in red.

2. Present a card to the reader.
   Result: The LED should light briefly in green and the reader should sound a short beep. This indicates that the reader recognized the card.

3. Depending on the setup of the controller database for the card used in the previous step, one of two events will occur within a second of the beep in step 2. Note that either response indicates that the reader is working.
   – If the card is configured in the controller's database to allow access through the reader, then the LED will light in green for few seconds indicating that access has been granted.
   – Or, if the database has not yet been configured, then the LED will flash between red & green in a rapid alternating pattern for two to three second indicating that access has been denied.

The above tests validate that the reader is functioning correctly.

If installing a keypad type reader, then you will need to further configure the reader database before you can properly validate keypad operation. Refer to the Software Manual for information of configuring the reader database to support card and PIN operating. After making necessary database updates, the keypad can now be tested as described in the next section.



BELDEN 9944 Equivalent
RED
BLACK
GREEN
WHITE
ORANGE

HID PROXPRO Pigtail	
1	+12 VDC
2	Ground
3	Data 0
4	Data 1
5	Green LED
6	Red LED
7	Beeper
8	Hold
9	Tamper Common
10	Tamper Select

9.4 HID ProxPro Reader with Keypad

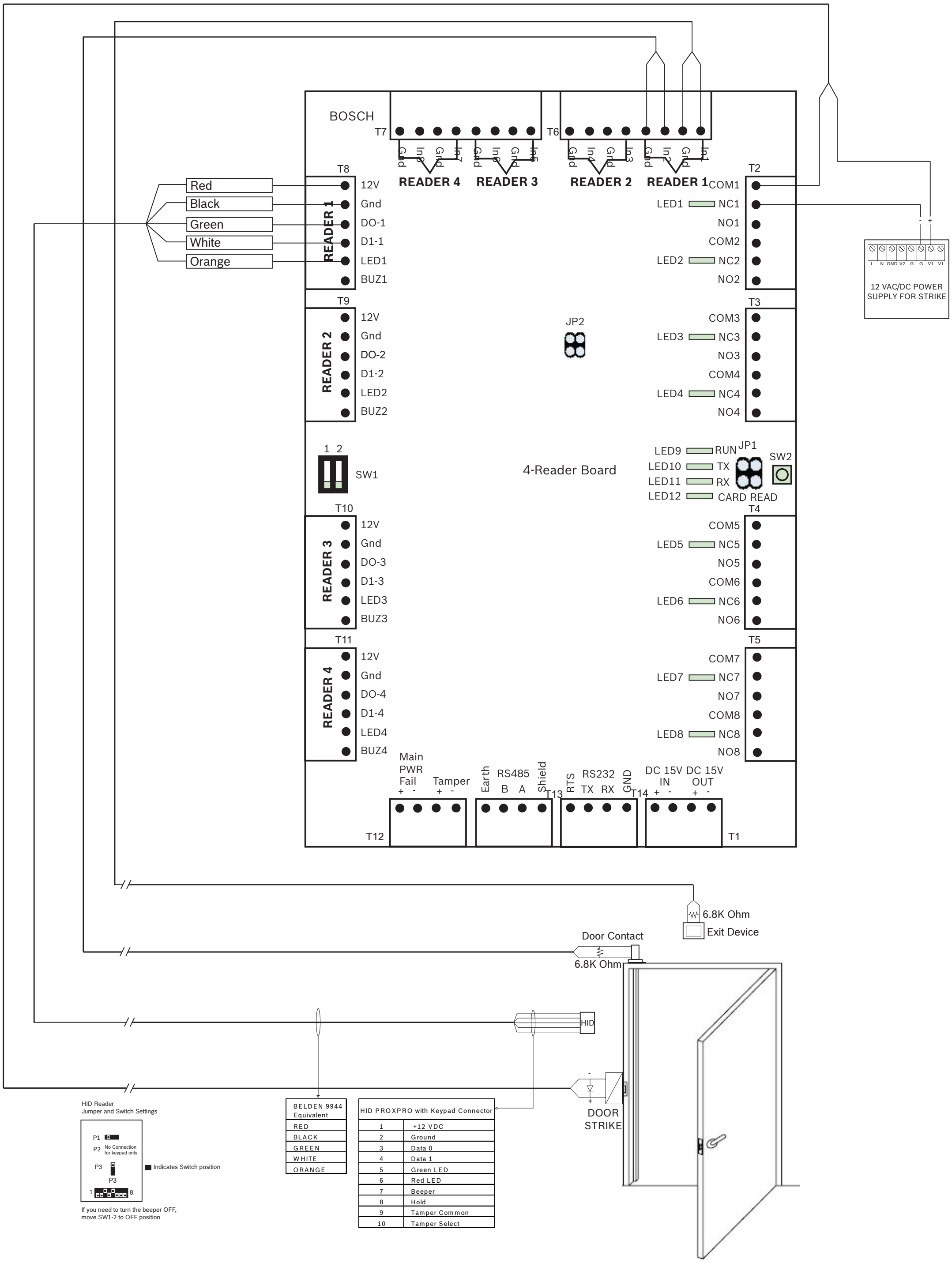
1. Make necessary database updates as described in the previous paragraph to configure the reader for card and PIN operation.

2. Present a card to the reader.
   Result: The LED should light briefly in green and the reader should sound a short beep. This indicates that the reader recognized the card.

   The reader LED should then begin a slow alternating flash between red and green indicating that the PIN code should be entered.

3. Enter the card's PIN code by slowly pressing the numeric keys on the reader's keypad. After entering the last digit, press the # key to complete PIN entry.
   Result: An audible beep will be heard after each key is pressed.

4. Depending on the setup of the controller database for the card used in the previous step, one of two events will occur within a second after pressing the # key in the previous step. Note that either response indicates that the reader and keypad are working.
   - If the card is configured to allow access through the reader and the correct PIN code was entered, then the LED will light in green for a few seconds indicating that access has been granted.
   - Or, if the database has not yet been fully configured, then the LED will flash rapidly in an alternating pattern between red & green for two of three seconds indicating that access has been denied.



BELDEN 9944 Equivalent
RED
BLACK
GREEN
WHITE
ORANGE

HID PROXPRO with Keypad Connector	
1	+12 VDC
2	Ground
3	Data 0
4	Data 1
5	Green LED
6	Red LED
7	Beeper
8	Hold
9	Tamper Common
10	Tamper Select

9.5 Field Devices using IO Board

This will provide the system installer to have the flexibility of configuring any input in the panel to be in any monitoring requirement. The diagram below shows the wiring diagram for 2 State Non-Supervised, 2 State Supervised and 4 State Supervised input points.

9.5.1 Wiring Diagram for Supervised Inputs

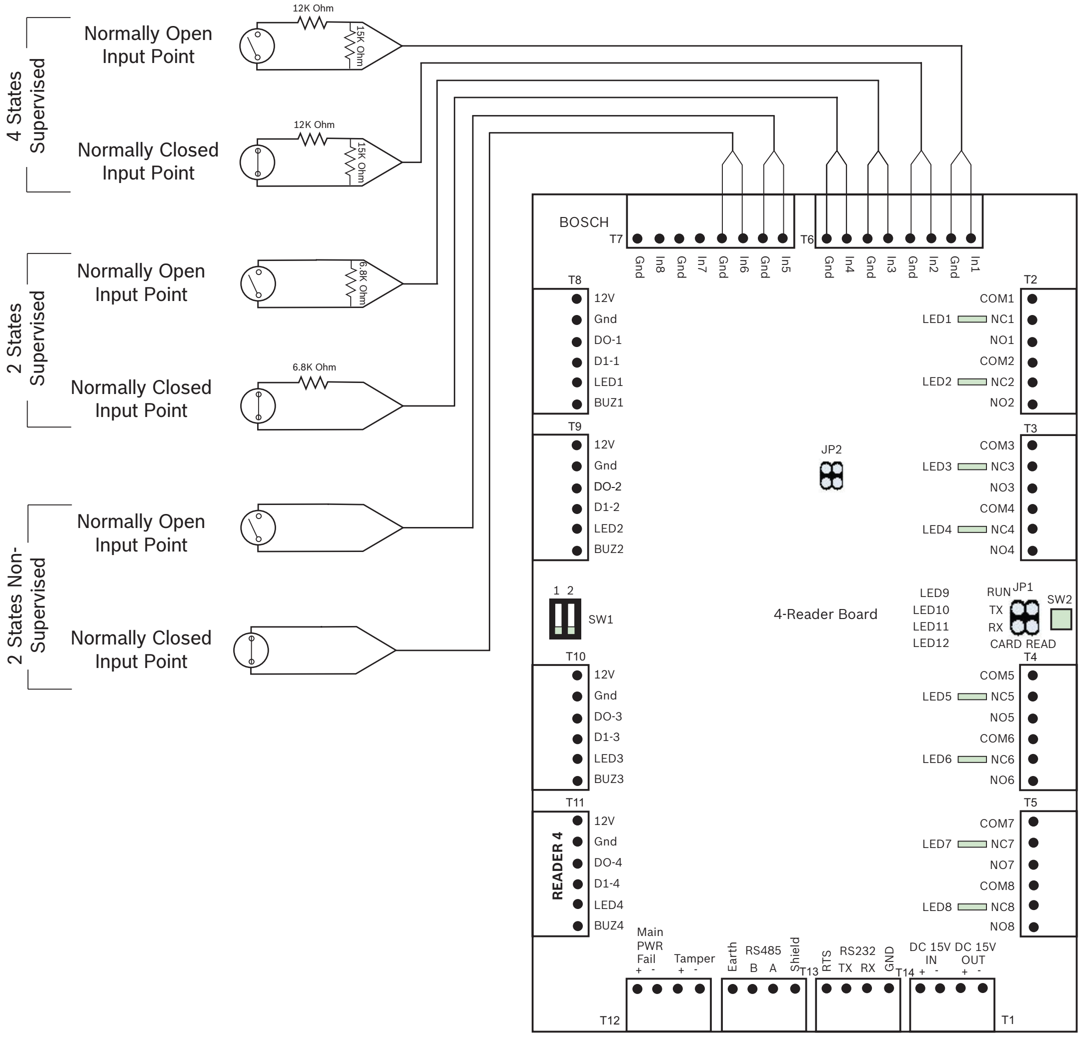

4 States Supervised
Normally Open Input Point
12K Ohm
15K Ohm
Normally Closed Input Point
12K Ohm
15K Ohm
2 States Supervised
Normally Open Input Point
6.8K Ohm
Normally Closed Input Point
6.8K Ohm
2 States Non-Supervised
Normally Open Input Point
Normally Closed Input Point
BOSCH
T7
Gnd In8 Gnd In7 Gnd In6 Gnd In5
T6
Gnd In4 Gnd In3 Gnd In2 Gnd In1
T8
12V Gnd DO-1 D1-1 LED1 BUZ1
T9
12V Gnd DO-2 D1-2 LED2 BUZ2
T10
12V Gnd DO-3 D1-3 LED3 BUZ3
T11
READER 4
12V Gnd DO-4 D1-4 LED4 BUZ4
T2
COM1 NC1 NO1 COM2 NC2 NO2
LED1 LED2
T3
COM3 NC3 NO3 COM4 NC4 NO4
LED3 LED4
T4
COM5 NC5 NO5 COM6 NC6 NO6
LED5 LED6
T5
COM7 NC7 NO7 COM8 NC8 NO8
LED7 LED8
JP2
1 2
SW1
4-Reader Board
LED9 LED10 LED11 LED12
RUN JP1 TX RX CARD READ
SW2
Main PWR Fail + -
Tamper + -
Earth RS485 B A Shield
T13 RTS RS232 TX RX GND
T14 DC 15V IN + - DC 15V OUT + -
T12
T1

Figure 9.1 Wiring Diagram for Supervised Inputs

10 How to Install the Access Easy Controller 2.1

10.1 Preliminary

1. You will need to obtain the mounting location details from the customer before the controller can be installed.
   The mounting location of the controller should provide:
   a. protection from unauthorized access
   b. protection from accidental damage
   c. (ideally) an uninterruptable power supply
   d. protection from electrical interference
   e. an environment temperature range of 0°C - 50°C
   f. an environment humidity of 5% ~ 85% +/-5% RH
   g. a network connection point - either a wall jack or an available hub where a category 5 cable can be plugged in, to provide the AEC2.1 with access to the customer's network.

2. The customer will also need to provide some additional information before the controller can be made operational.
   a. An IP address for the controller
   b. The subnet mask to be used by the controller.
   c. If a gateway is used by the customer's network, then obtain the gateway address to be used by the controller.
   d. E-mail server IP address, port number, and domain name (required only if the customer intends to use the controller's e-mail notification services).
   e. Location of an analog telephone line (required only if a dial-in connection will be used).

NOTICE!
If the AEC2.1 is going to be directly connected to a host computer on its own private network, and not to the customer's company network, then the controller's default IP address setting (192.168.0.41) can be used.

3. For a UL-compliant installation, adhere to the following installation guidelines:
   a. The controller must be installed in the same room as the network jack or hub.

10.2 Mounting the Panel on a Concrete Wall

This section addresses the mounting of the AEC2.1 panel. For mounting always use hardware and materials appropriate to the nature of the surface upon which the panel is mounted. The following instructions describe the basic steps to mount the panel on a concrete wall.

WARNING!
For mounting always use hardware and materials appropriate to the nature of the surface upon which the panel is mounted. If in doubt, consult a certified technician.

1. After acquiring the exact mounting location, mark out the exact position of the mounting holes.
   a. Place the panel against the wall, over the area where the panel is to be mounted.

   b. Use a marker to mark out the exact position of the mounting holes from the panel. Make sure that the panel is held firmly in place before marking out is done.

2. Drill on the marked out position on the wall.
   a. Use a concrete drill bit with a hammer drill for drilling on a concrete wall.
   b. Ensure drill bit is placed perpendicular to the wall surface before commencing drilling. Drilled hole should be perpendicular to the wall surface.
   c. Drilled hole should be such that a stainless steel sleeve anchor bolt can be fully inserted into the hole.

3. Insert the stainless steel sleeve anchor bolt into the drilled hole and tighten the nuts to mount the panel in place.
   a. Use a hammer to lightly hammer the bolt in.
   b. Place the panel over the bolts, place a flat washer follow by a spring washer before tightening each nut to fix the panel in place.

WARNING!
The bolt should fit snugly in the drilled hole. Do not mount the panel on a bolt that is loose in the drilled hole.

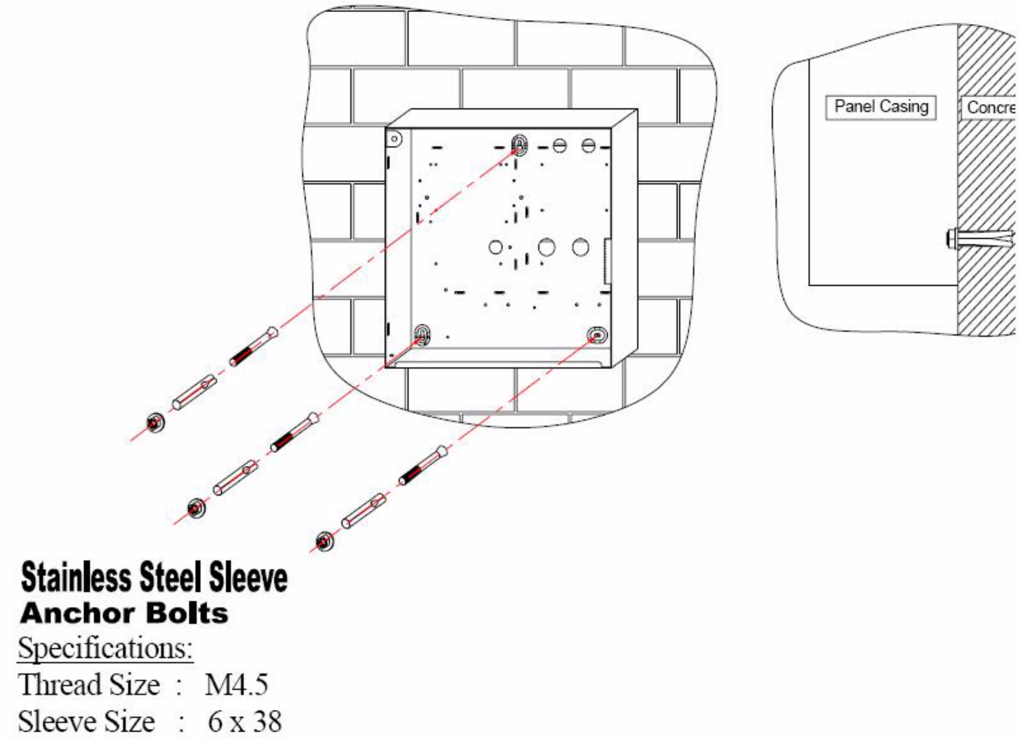


Figure 10.1 AEC fixing procedure

NOTICE!
The Dimensions of the Stainless Steel Sleeve Anchor Bolt:Sleeve Size: 6 x 38mmMin. Hole Depth: 35mmFixing Hole Dia.: 6mmThread Size: M4.5

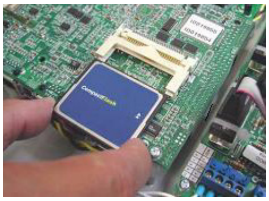
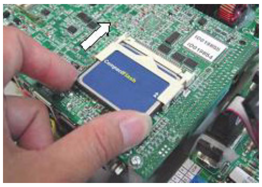
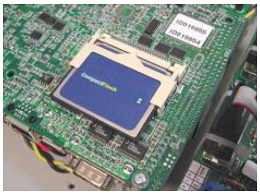
10.3 Controller Installation

Installation and wiring must be done in accordance with all applicable electrical and safety codes

1. Mount the controller and strike/lock power supply.
   - Remove any necessary knockouts from the top and/or back of the AEC2.1 enclosure to provide access for wiring.
   - Install conduits as needed to protect wiring.
   - Connect the power cable (100~240 VAC) to the AEC2.1 power socket, but do not switch on the power.
   - Wire AC power to the strike/lock power supply.
   - Pull all required wiring from the controller to field device location.

2. Inspect all circuit boards
   - Check all circuit board mounting screws for snugness.
   - Verify that socket mounted components are secure.
   - Verify jumper and switch settings of all boards.

3. Insert Compact Flash onto the AEC2.1 CPU.
   - Follow the steps below to insert the Compact Flash onto the CPU board.

	1. Position the Compact Flash in the correct orientation.
	2. Slot in the Compact Flash as shown.
	3. Make sure the Compact Flash is fully inserted.

4. Install any needed expansion boards.
   - Mount boards in enclosure.
   - Install RS485 cables.
   - Install power cables.
   - Set jumpers and switches on boards.

5. Apply AC power to controller.
   - The power LED on the panel should light up, indicating that the panel is powered.
   - The CPU board should perform a power-up self-test.

NOTICE!
This test will take about 90 seconds to complete.

6. When booting up is completed, LEDs 10 and 11 on the interface boards will flicker. This indicates that the interface boards are communicating with the CPU. Also, the sounder on the CPU board will activate.
   - Install and connect the backup battery. Use a 12V, 7.0AH battery to provide four hours of standby power as required by UL.
   - Use a rubber band or a piece of tape to temporarily close the enclosure tamper switch. This should silence the sounder.

This completes the basic controller installation. Refer to *Section 13.5 How to Set Initial Controller Configuration, page 74* for instructions on setting the controller's IP address.

NOTICE!
AEC2.1 uses RS485 multi-drop communication channels between the interface boards. An end-of-line jumper is to be added on the last interface board of the configuration to stabilize the communication.

The figure below shows the inter-connection of the Main Controller panel.

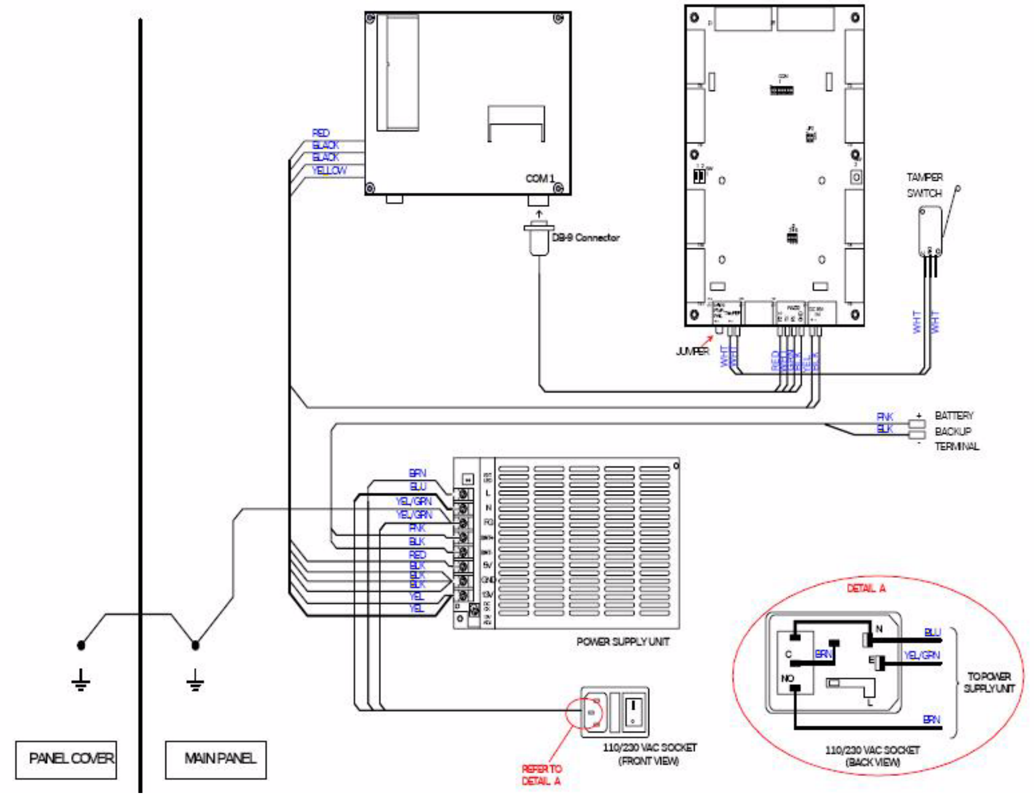


Figure 10.2 Inter-connection of the components within the main controller panel

11 Card Reader Keypad Functions

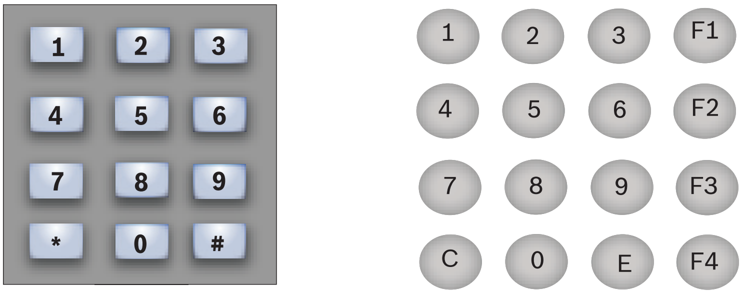
AEC2.1 supports a range of Card Readers for different card types that is suitable for use in AEC2.1 Panel.

Some Card Readers come with built-in Keypad that is most suitable for use as Entry reader. Depending on the model selected, the Keypad could be either a 3X4 or a 4X4 buttons layout.

This Chapter explains the function(s) of the key or a combination of keys on the Keypad.

11.1 Keypad Layout

The figure below shows two typical keypad layouts for card reader units. The size and shape of the keypad may be different depending on the type of card reader units.



3X4 Keypad

4X4 Keypad

Figure 11.1 Keypad Layouts

11.1.1 Keypad Functions

For the 3x4 matrix keypad, each numeric key is also used as special function key. The special function keys are described below.

For the 4x4 matrix keypad, there are 4 dedicated function keys. However, each numeric key is also used as special function key. The special function keys are described below.

1. The F4 or 2 key is used for changing PIN code.

2. The 4 key is used to allow manual card number entry.

3. The 5 key is used in order for the system to capture the clock-in times of the cardholders (employees and guards).

4. The 6 key is used in order for the system to capture the clock-out times of the cardholders (employees only).

5. The # or E key is used to terminate an entry.

6. The * or C key is used to cancel/quit any changes made.

7. The 0 key is used together with an arming card to arm an alarm zones.

11.2 Entry Operation

The following sections highlight the various means to enter and exit a controlled area using the keypad. These functions MUST be enabled in the Card Reader parameter setting before it could be used. Refer to the AEC2.1 Software manual for details in enabling these functions.

11.2.1 Using Card + PIN Mode on a Keypad Reader

Follow the procedure below to gain access:

1. Present the card to the Reader, the LED will flash at a slow rate for the duration as depicted in the Reader's Keypad Time-out field.

2. Enter your PIN code. If the PIN code is valid, pull the door to get in. Otherwise, the LED will flash at a fast rate, indicating a wrong PIN code.

11.2.2 Using Keypad in “Enable Keypad Only Operation” Mode

If the Enable Keypad Only Operation mode is activated, all users can either gain access by presenting card or by entering their card number using the 4 key. However, if the card(s) is set in Card and PIN operation AND the door requires PIN code for entry, user(s) have to enter their card number followed by their assigned PIN code before access is granted.

Manual Card Entry without PIN code

1. First, press the 4 key, The LED will flash continuously at a slow rate for the duration as depicted in the Keypad Time-out field.

2. Key in your card number followed by the # or E key. If the card number is valid, the door will be released momentarily for access. However, if the card number is not valid, the LED will flash at a fast rate.

Follow the next set of procedures if PIN code is required.

Manual Card Entry with PIN code

1. First, press the 4 key, The LED will flash continuously at a slow rate for the duration as depicted in the Keypad Time-out field.

2. Key in your card number followed by the # or E key. If the card number is valid, the LED will flash at a medium rate. However, if the card number is not valid, the LED will flash at a fast rate.

3. Enter the PIN code. If the PIN code is correct, the door will be released momentarily for access. However, if the PIN code is wrong, the LED will flash at a fast rate.

Reader's PIN code

When this mode is selected, all cardholders use a pre-determined Reader's PIN code to gain access. No card is required. This setting is done in Card Readers, PIN Code Settings, Reader's PIN code (1-7 digits). To gain access, enter the Reader's PIN code.

11.2.3 Other Usage

The following sections highlight the other usage of the Reader beside Door Access.

Time Clock Functions

Besides using the card for door access, it can be used for time clocking. For example, an employee reports for work will be granted access to the building at the same time, the employee can clock-in. These transactions are captured and presented in the Time Attendance web page which can be exported in Comma Separated Variable (.csv) format and can be used by third party payroll software. The function can also be used to capture the time, the guards visited the checkpoint.

NOTICE!

No set-up is required in the AEC2.1 web page.

To Clock In

Press the 5 key of the Entry Reader and present your card. The LED will flash once and the door will be unlocked if the cardholder has been given the access right.

To Clock Out

Press the 6 key of the Entry Reader and present your card. The LED will flash once. The door remains locked.

If presenting card without pressing any one of these two keys, the reader will resume normal door access operation. There will not be any Clock In or Clock Out transactions.

11.2.4 Changing PIN Code

The PIN code can be changed by first activating the 2 or F4 key before presenting the card. General steps to change the PIN code.

1. Press the 2 or F4 key.

2. Present Card - LED will flash at a slow rate.

3. Enter the old PIN code - LED will flash at medium rate.

4. Enter the new PIN code - LED will stop flashing.

5. Press # or E key (PIN code change is completed).

For example, suppose you want to change an old PIN code (8088000) to a new PIN code (4321).

1. First, press 2 or F4 key.

2. Present your card to the Reader. The LED will start to flash continuously at a slow rate for the duration as depicted in the Keypad Time-out field.

3. Enter the old PIN code 8 0 8 8 0 0 0, the LED will flash continuously at medium rate. However, if the entered PIN is wrong, the LED will flash continuously at a fast rate. In this case, press * or C and repeat from step 1.

4. Enter the new PIN code 4 3 2 1, followed by # or E key.

5. Press the # or E key to complete the process.

NOTICE!
The number of digits for the User PIN code range from 1 to 7 digits. Refer to the AEC2.1 Software user manual chapter on Card Administration > Card Functionality for further details.

11.2.5 Entry and Arm/Disarm Reader

A Reader can be configured to allow arming or disarming a group of Input Points (collectively called an Alarm Zone), using methods similar to Door Access such as, Manual Card Number entry, Card only, Card + PIN code and common Reader's PIN code (refer to the previous section for detail).

Cardholders can arm/disarm the Alarm Zone and this setting is configured under the section Card Administration, Card Functionality.

The statuses of the Alarm Zone are indicated via the LED.

HID reader LED indicators

HID reader	**LED**	**Buzzer**
Armed.The zone is Armed	Red	Off or Beeping During Arm Delay
Part ArmedThe zone is Armed with some Input Point(s) bypassed. Card is presented to the Reader when the LED is flashing.	Green/Red Alternating at slow rate	Off or Beeping During Arm Delay

HID reader	LED	Buzzer
Ready/DisarmedAll Input Points in the zone are in the Normal state and are ready for Arming.	Green	Off
Not Ready/DisarmedOne or more Input Points is not in the Normal state and not ready for Arming	Green/Red Alternating at medium rate	Off
AlarmThe zone is Armed and one or more Input Point is in Alarm State	Red	0.5 sec. On and 0.5 sec. Off

*Slow flashing is at around 1 sec. ON then 1 sec. OFF interval; whereas normal flashing is at ½ sec. interval.

The LED besides being used to indicate an alarm condition in the zone is also used during the Arming process.

When you arm the Alarm Zone, the LED will flash for the duration as depicted in the Arm Delay field of that particular Alarm Zone. We provide a few example below for further understanding.

Configuration in the AEC2.1
- Input Points #1, 2, 3, and 4 are grouped as Alarm Zone #1.
- Arm Delay = 15 seconds.
- Alarm Delay = 0 seconds
- Reader #4 is the Arm/Disarm Reader for Alarm Zone #1.
- Some cards are given the access rights to arm/disarm Alarm Zone #1. No PIN code required.

Arming an Alarm Zone

Example 1 - All Input Points are in the Normal state.

1. LED has a stable green light.
2. Press 0 key and present the arming card to Reader #4.

LED turns to red light.

Buzzer will beep at a fast rate for 15 seconds.

The Alarm Zone is ARMED.

In the Transactions web page, you should see the Armed transaction as carried out by the particular card number, user name, time, date and location of reader. The status of the Input Points is also shown on the Input Control web page.

Example 2 - Input Point #1 is in Normal State, while Input Point #2 is in the Open state.

1. LED is flashing (Green/Red) in medium rate; indicating one of the input is in open state.

2. Press 0 and present the arming card to Reader #4, to arm the Alarm zone.

LED is flashing (Green/Red) in slow rate

Buzzer will beep at a fast rate for 15 seconds.

The Alarm Zone is ARMED with Input Point #2 “bypassed”.

In the Transactions web page, beside seeing similar transaction to Example 1, there will be a Bypassed transaction for Input Point #2. The “bypassed” status for Input Point #2 is also shown in the Input Control web page.

Example 3: Alarm zone 1 is armed.

1. LED has a stable red light.

2. When any one input is activated, the buzzer will beep in a low rate continuously.

3. Present the disarming card to the reader.

Buzzer stop.
LED turns to green light
The Alarm Zone is DISARMED.

Disarming an Alarm Zone
To disarm an Alarm Zone, just present the arming card to the Reader.

12 Common Alarm Output

12.1 Overview

The AEC2.1 provides a Common Alarm output that can be used to provide a hand-off to an extended alarm system, whenever an alarm condition is detected by the controller.

The Common Alarm output is available from the last relay on the first 4-Reader board. The output consists of Form-C type dry contacts rated to handle 1A @ 24 VDC Resistive. Refer to *Figure 5.2, Page 20* for wiring information on the Common Alarm output.

The Common Alarm output will activate automatically whenever the AEC2.1 detects any of the following conditions:

- Door Forced Open is detected from a reader controlled door,
- Door Held Open is detected from a reader controlled door,
- Alarm is detected from an input point on an 8-IO board,
- AC Power Failure to controller is detected,
- Controller Tamper is activated, or
- Duress condition is signalled from a keypad reader.

Once activated, the Common Alarm output will remain activated until the condition that caused alarm returns to normal. In the event multiple alarms exist within the controller, the Common Alarm output will remain activated till all alarm conditions are restored.

A duress condition is an exception to the processing explained in the previous paragraph. The Common Alarm output will activate immediately when any cardholder of a card reader, signals a duress situation from the reader's keyboard. But, because a duress event does not have a restoration associated with it, the Common Alarm output will remain activated until the duress alarm is acknowledged from the transactions screen.

The headings below describe the type of alarm that will trigger the Common Alarm output.

12.2 Alarm (All Input Points)

These Input Points, ranging from address 33 to 64, when Armed by schedules or manually through a dedicated Arm/Disarm Reader or through the web page could monitor the input status.

Once triggered, the Common Alarm Output will be turned on until the Input Point is restored or the input is Disarmed.

12.3 Door Forced Open and Door Held Open

These two transactions are related to the 32 Readers (Doors). When there be such a transaction, the Common Alarm Output triggers and is restored when the Door Contact is closed i.e. the door is closed.

12.4 Panel AC Failure

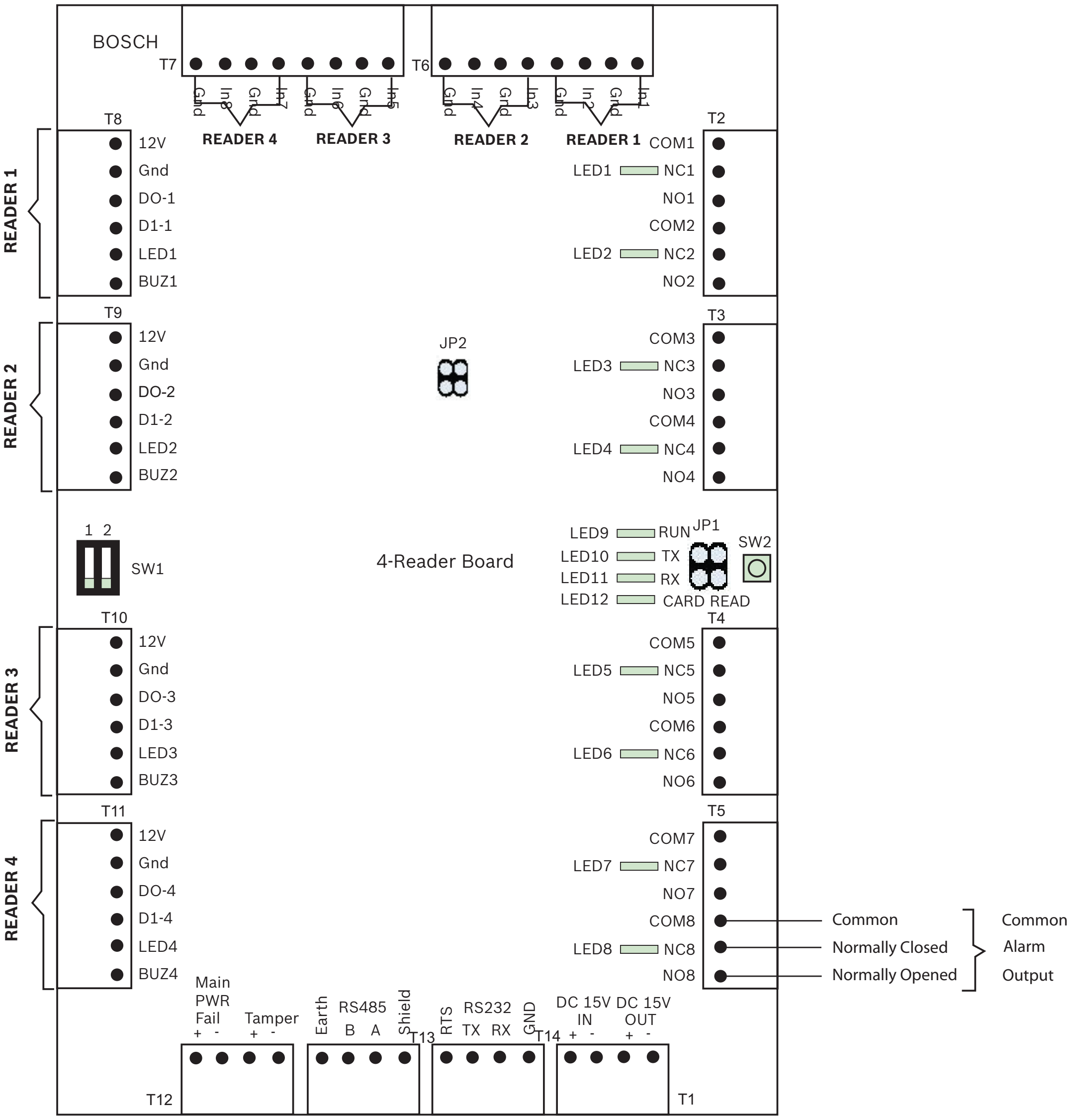
When there is a power outage and the controller is taking power from the backup battery, the message Panel AC Failure, is sent to the Transactions web page. The Common Alarm Output is triggered on and is restored when the main power supply is restored.

12.5 Controller Tamper

Everytime the Controller's cover is opened, the message Controller Tamper is sent to the Transactions web page. The Common Alarm Output is triggered on and is restored only when the Controller's cover is closed back.

12.6 Duress

Whenever a cardholder activates a duress code, the message Duress is sent to the Transactions web page. The Common Alarm Output is triggered on and is restored only when the AEC2.1 software user acknowledges the duress alarm transaction in the Transactions web page.



13 How to Set Up the Access Easy Controller 2.1 and the Computer

This chapter provides the basic setup and configuration details of the AEC2.1 system. It is to be used together with the AEC2.1 Software Manual for a complete configuration of the system.

13.1 Overview

This section describes the steps required to connect the AEC2.1 system to the customer's network. It also summarizes the configuration steps needed on a computer for the computer to be able to connect to the AEC2.1.

NOTICE!
AEC2.1 is for indoor use only and the system must be installed indoors within the protected premises.

AEC2.1 Set-up

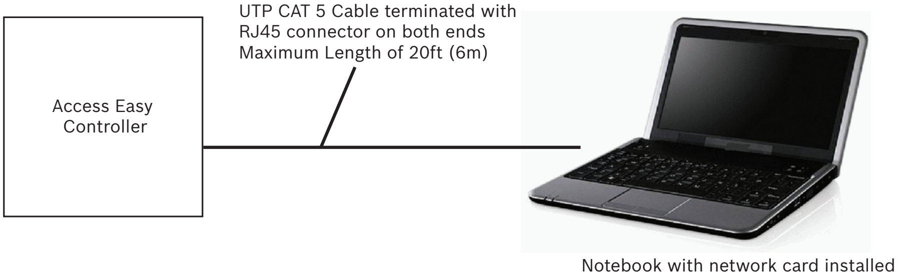
All AEC2.1 are shipped from the factory with default IP address of 192.168.0.41. Before the controller can be connected to the customer's network, its IP address will need to be changed to fit into the customer's network configuration.

If the controller is going to be connected directly to a stand-alone computer on its own private network, the controller's default address need not be changed. All that will be necessary is to configure the computer's network settings so that it has an address on the same network as the controller

For initial setup of the AEC2.1, a Notebook or Desktop computer will be required. The computer used for the controller setup must have a 10/100Base-T Ethernet card installed in it, and must run a WindowsXP/Vista or Mac operating system. The computer must also have a functional Web browser program, such as Microsoft Internet Explorer, version 7.0.

1. Configure the computer that is to be used for setting the controller's IP address so that it has an IP address on the same 192.168.0 network as the controller. We suggest you set the computer's IP address to 192.168.0.40, and the subnet mask to 255.255.0.0.
   (If you are not sure how to change a computer's network settings, refer to *Section 17 Appendix A How to Install & Set the TCP/IP Address on a PC, page 91*).

2. Connect the AEC2.1 to the computer using a standard Cat-5 crossover cable (Beige Cat-5 cable) as shown below.


UTP CAT 5 Cable terminated with
RJ45 connector on both ends
Maximum Length of 20ft (6m)
Access Easy Controller
Notebook with network card installed

3. Follow the directions in the section of this manual entitled *Section 13.5 How to Set Initial Controller Configuration, page 74*.

NOTICE!
The AEC2.1 is a stand alone system and does not require a constant connection to a PC for proper operation. The PC is used as a programming or downloading tool.

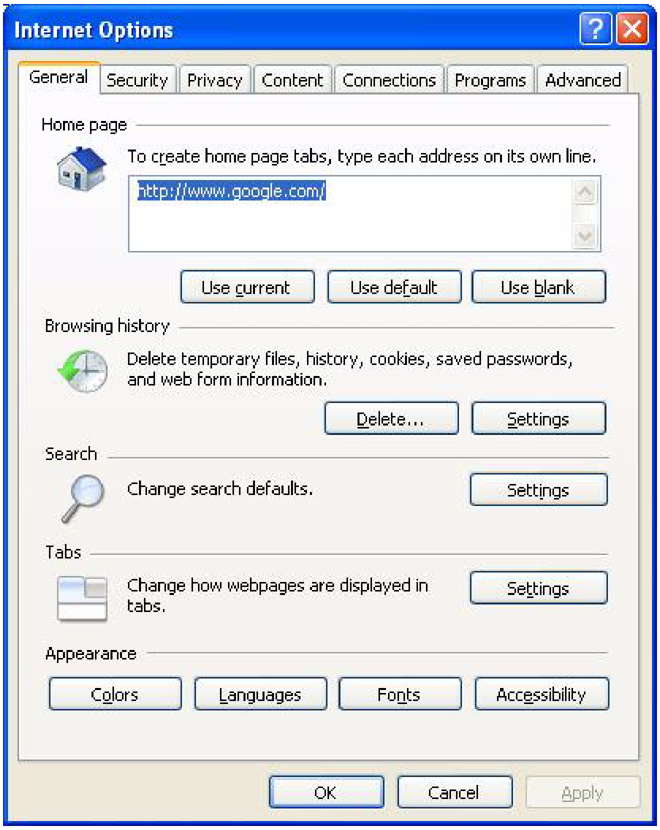
13.2 Configuring a Web Browser to Work with Access Easy Controller 2.1

The instructions in this section describes the steps necessary to configure the Web browser to operate with the AEC2.1. In most instances, you will not need to make any changes to the setup of a Web browser to connect to an AEC2.1. The guidelines presented in this section are intended for first-time browser users and as a technical reference if difficulty is encountered when connecting with an AEC2.1.

13.3 Web Browser Set-up on a Windows Computer

Follow the steps below to configure Microsoft's Internet Explorer version 7.0 or above. Other Web browsers are also similar.

1. Click on **Start** > **Settings** > **Control Panel**. From the Windows Control Panel, click the Internet Options **Internet Options** icon. The screen below appears.



Internet Options

Home page

To create home page tabs, type each address on its own line.

http://www.google.com/

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

Search

Change search defaults.

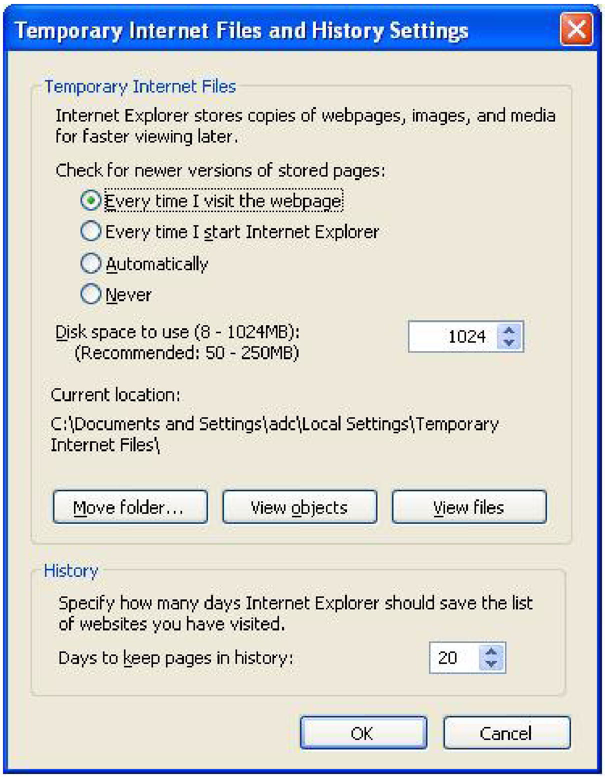
Tabs

Change how webpages are displayed in tabs.

Appearance

2. If you want the AEC2.1 login page to open every time you activate your Web browser, then set the Home page Address to the AEC2.1's assigned IP address in the **Address** field.

3. Under Browsing History, click the Settings... **Settings** button to display the settings dialog box as shown below. Confirm that the option in **Check for newer versions of stored pages** is set to **Every Time I visit the webpage** as shown below. If it is not, select the corresponding radio button to select this option. This step is necessary to update the 'Activity' user interface menu and to transfer the images from the server to the system periodically. The '**Activity** > **Transactions**' menu lists all the activities performed by the AEC panel.



Temporary Internet Files and History Settings

Temporary Internet Files

Internet Explorer stores copies of webpages, images, and media for faster viewing later.

Check for newer versions of stored pages:

● Every time I visit the webpage
○ Every time I start Internet Explorer
○ Automatically
○ Never

Disk space to use (8 - 1024MB): (Recommended: 50 - 250MB) 1024

Current location:

C:\Documents and Settings\adc\Local Settings\Temporary Internet Files\

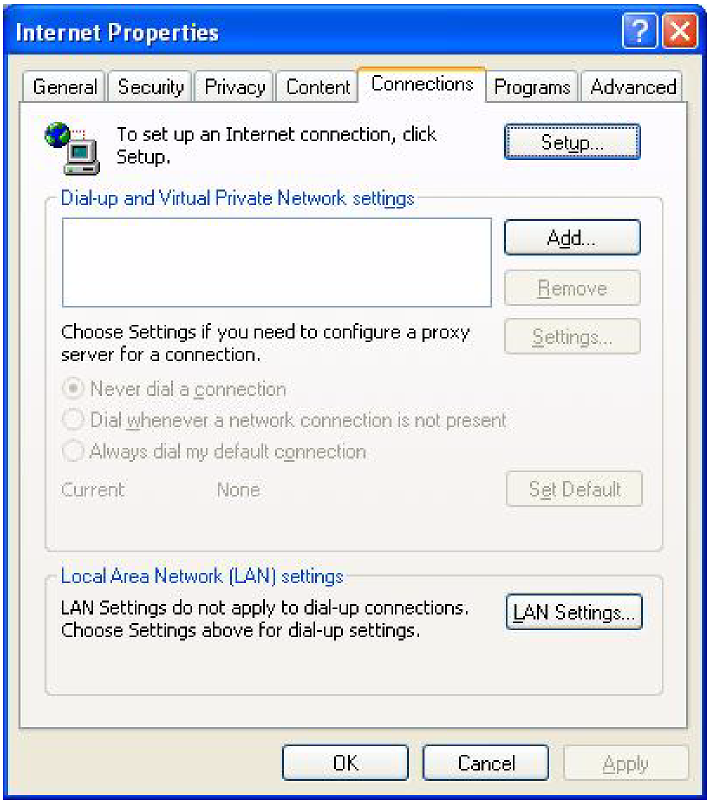
History

Specify how many days Internet Explorer should save the list of websites you have visited.

Days to keep pages in history: 20

4. Click the OK button to save the changes and exit from the Settings windows. You will return to the **Internet Option** dialog box as shown in point 1.

5. From the **Internet Option** screen, select the **Connections** tab to display the Connections dialog box. This screen below appears.



To set up an Internet connection, click Setup.

Choose Settings if you need to configure a proxy server for a connection.

● Never dial a connection

○ Dial whenever a network connection is not present

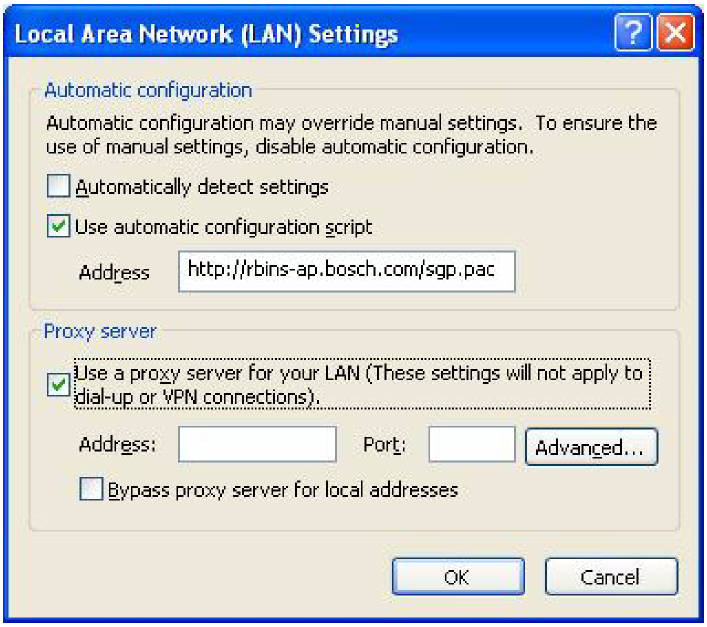
○ Always dial my default connection

Current None

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings.

6. Click LAN Settings... to display the LAN Settings dialog box.

7. If your network does not use a proxy server, then you can skip and go directly to step 10. If your network does use a proxy server, then select **Use a proxy server for your LAN** in the **Proxy Server** window as shown below.



Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☐ Automatically detect settings

☑ Use automatic configuration script

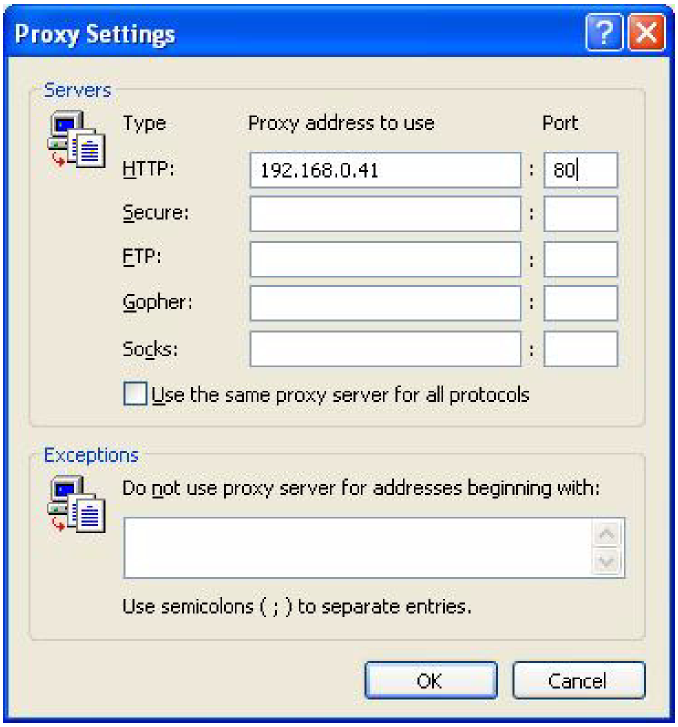
Address http://rbins-ap.bosch.com/sgp.pac

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port:

☐ Bypass proxy server for local addresses

8. In the **Proxy Server** window click the **Advanced** button to show the **Proxy Settings** dialog box. In the proxy settings dialog box enter the IP address of the AEC2.1 as shown below.


Proxy Settings

Servers

Type | Proxy address to use | Port

HTTP: 192.168.0.41 : 80

Secure: :

FTP: :

Gopher: :

Socks: :

□ Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

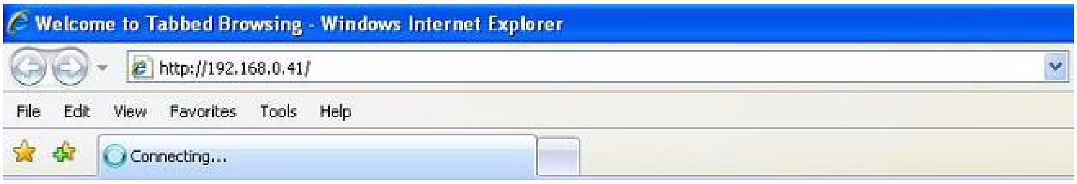
Use semicolons (;) to separate entries.

9. Click the OK button repeatedly to exit the Internet Options window. Then close the Control Panel.

10. Make sure you have a crossover type network cable connected between the computer and the AEC2.1. Now run the Web Browser program from Windows.

NOTICE!
You may receive a warning indicating that the page you are trying to reach is not available. Do not be concerned with this message at this time.

11. Enter the AEC2.1's IP address in the browser's Address box as shown below.

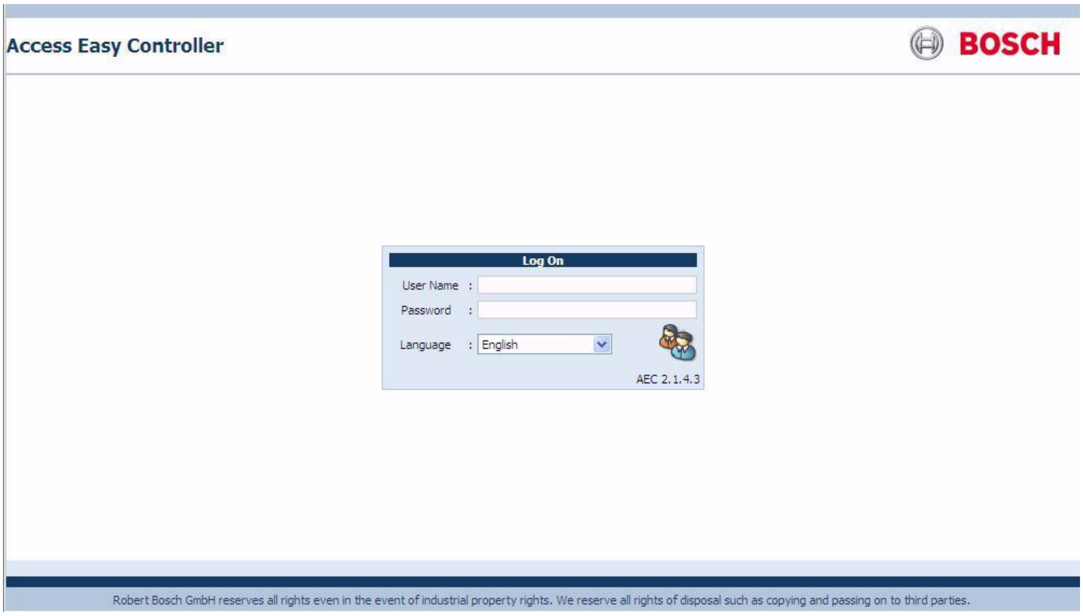

Welcome to Tabbed Browsing - Windows Internet Explorer

http://192.168.0.41/

Connecting...

Note: All screens are presented in Internet Explorer 7.0.

12. This will bring up the login page. The screen below shows the AEC2.1's login page.



User Name :

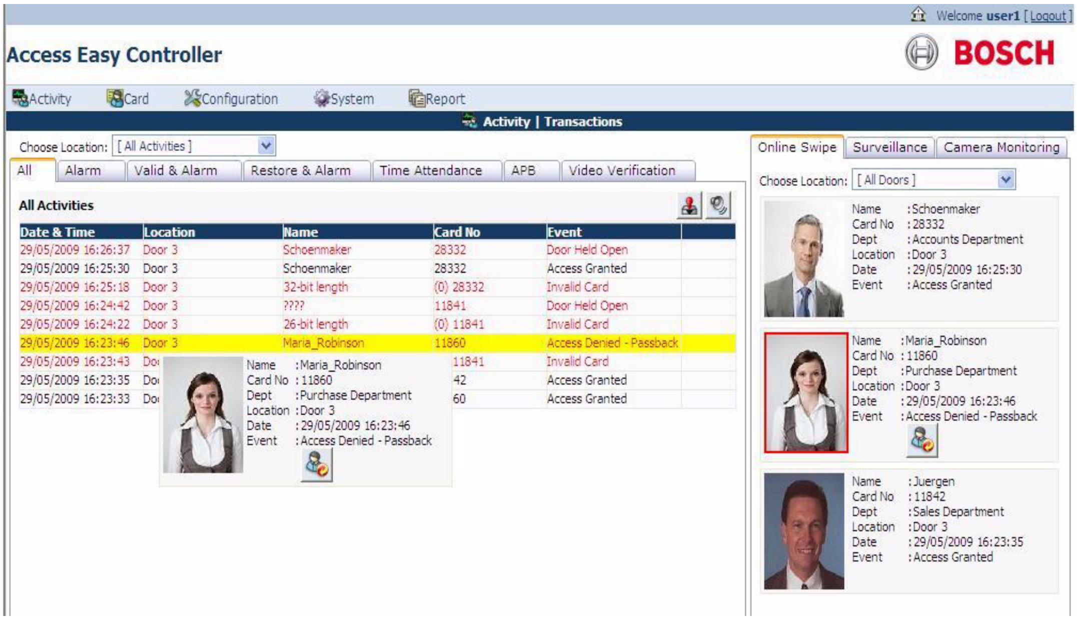
Password :

Language : English

Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

13. Proceed to login using the default user id: **user1** and password: **8088**. Select the required GUI language from the language dropdown. Upon successful login, the controller's home page is displayed as shown below.

NOTICE!
Changing the language in the login page changes the GUI language interface and not the database.



Choose Location: [All Activities]

All Activities

Date & Time	Location	Name	Card No	Event
29/05/2009 16:26:37	Door 3	Schoenmaker	28332	Door Held Open
29/05/2009 16:25:30	Door 3	Schoenmaker	28332	Access Granted
29/05/2009 16:25:18	Door 3	32-bit length	(0) 28332	Invalid Card
29/05/2009 16:24:42	Door 3	????	11841	Door Held Open
29/05/2009 16:24:22	Door 3	26-bit length	(0) 11841	Invalid Card
29/05/2009 16:23:46	Door 3	Maria_Robinson	11860	Access Denied - Passback
29/05/2009 16:23:43	Do		11841	Invalid Card
29/05/2009 16:23:35	Do		42	Access Granted
29/05/2009 16:23:33	Do		60	Access Granted

Name : Maria_Robinson
Card No : 11860
Dept : Purchase Department
Location : Door 3
Date : 29/05/2009 16:23:46
Event : Access Denied - Passback

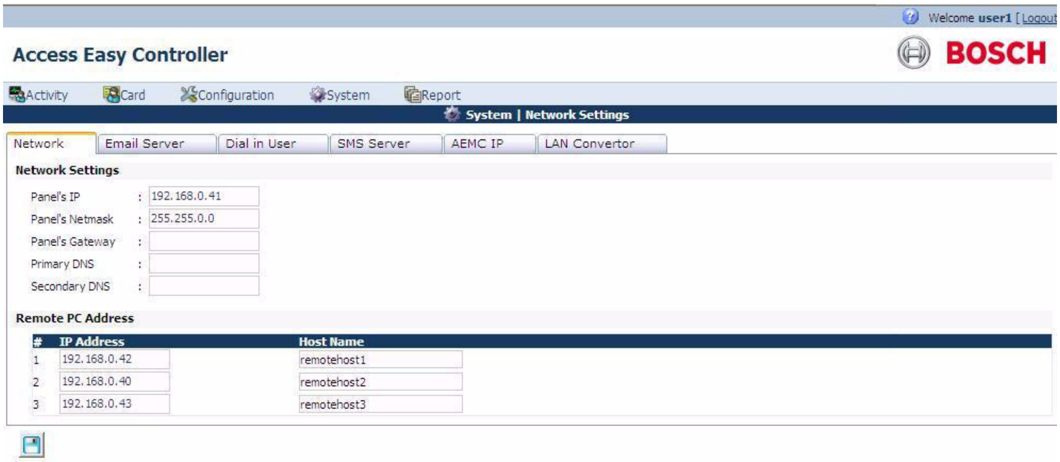
Choose Location: [All Doors]

Name : Schoenmaker
Card No : 28332
Dept : Accounts Department
Location : Door 3
Date : 29/05/2009 16:25:30
Event : Access Granted

Name : Maria_Robinson
Card No : 11860
Dept : Purchase Department
Location : Door 3
Date : 29/05/2009 16:23:46
Event : Access Denied - Passback

Name : Juergen
Card No : 11842
Dept : Sales Department
Location : Door 3
Date : 29/05/2009 16:23:35
Event : Access Granted

14. From the home page, select **System** > **Network Settings**. The Network Settings page appears. Make the required changes to configure the controller for operation on the customer's network. Click the save button to store the changes. Refer to the software manual for more information. The screen below shows an example of the settings made.



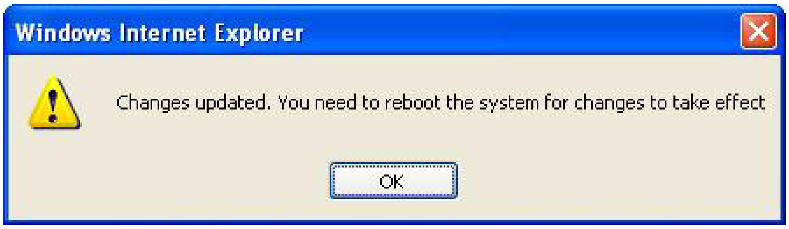
Network Settings

Panel's IP : 192.168.0.41
Panel's Netmask : 255.255.0.0
Panel's Gateway :
Primary DNS :
Secondary DNS :

Remote PC Address

#	IP Address	Host Name
1	192.168.0.42	remotehost1
2	192.168.0.40	remotehost2
3	192.168.0.43	remotehost3

15. After the database has been saved, the system will prompt you to reboot the controller as shown below. Click the **OK** button to reboot the controller. It will now boot using the new IP address. The controller is now ready to be connected to the customer's network.



Changes updated. You need to reboot the system for changes to take effect

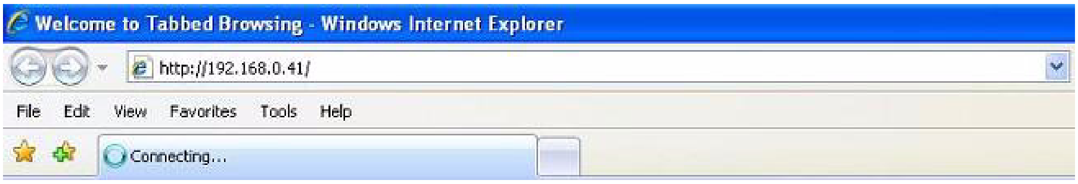
NOTICE!
For detailed information on database configuration, refer to the AEC2.1 Software User Manual.

13.4 Install AEC2.1 Certificate on a Windows Computer

Follow the steps below to install AEC2.1 certificate in Microsoft's Internet Explorer version 7.0 and above.

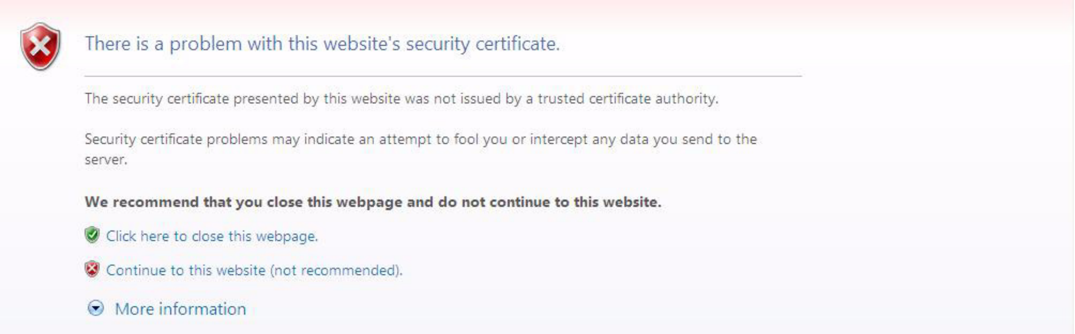
Note: The following steps should be followed if you are prompted with the certificate error message, if not this step should be skipped.

1. Enter the AEC2.1's IP address in the browser's Address box as shown below.



http://192.168.0.41/

2. This will bring up the certificate error page as shown below.



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

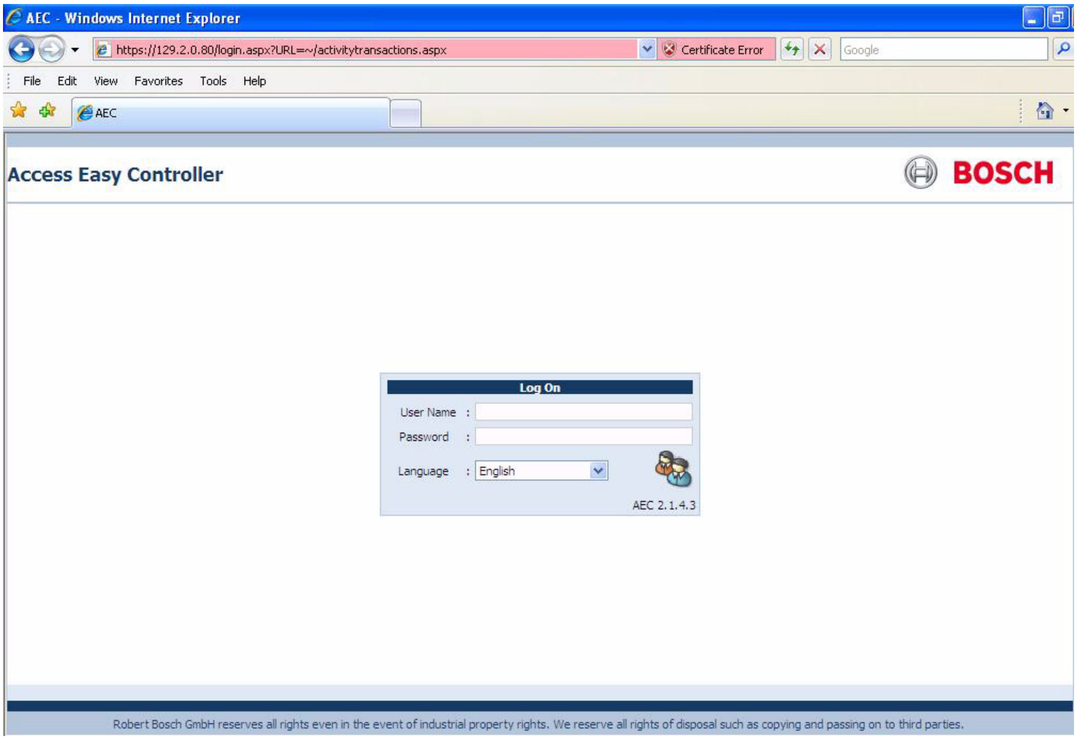
We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.

Continue to this website (not recommended).

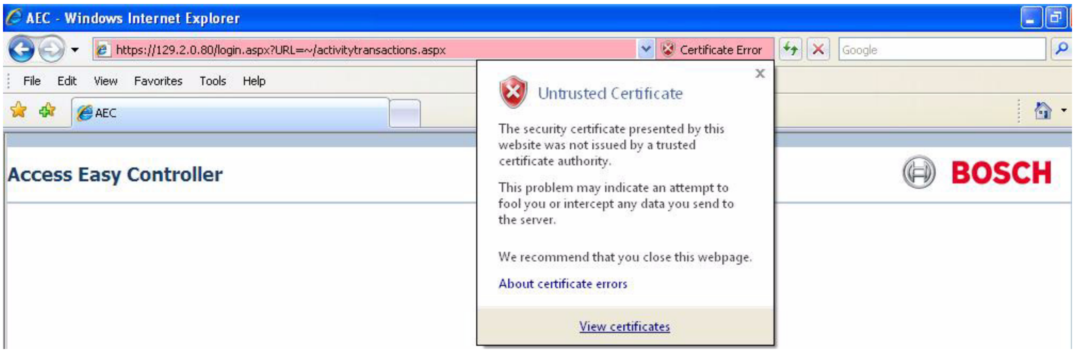
More information

3. Click on the link **Continue to this website (not recommended)**. This will bring up the login page with the certificate error message as shown below.



AEC - Windows Internet Explorer
https://129.2.0.80/login.aspx?URL=~/activitytransactions.aspx
Certificate Error
Google
File
Edit
View
Favorites
Tools
Help
AEC
Access Easy Controller
BOSCH
Log On
User Name :
Password :
Language :
English
AEC 2.1.4.3
Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

4. Click on **Certificate Error** message and click the **View certificates** link as shown.



AEC - Windows Internet Explorer
https://129.2.0.80/login.aspx?URL=~/activitytransactions.aspx
Certificate Error
Google
File
Edit
View
Favorites
Tools
Help
AEC
Access Easy Controller
BOSCH

Untrusted Certificate

The security certificate presented by this website was not issued by a trusted certificate authority.

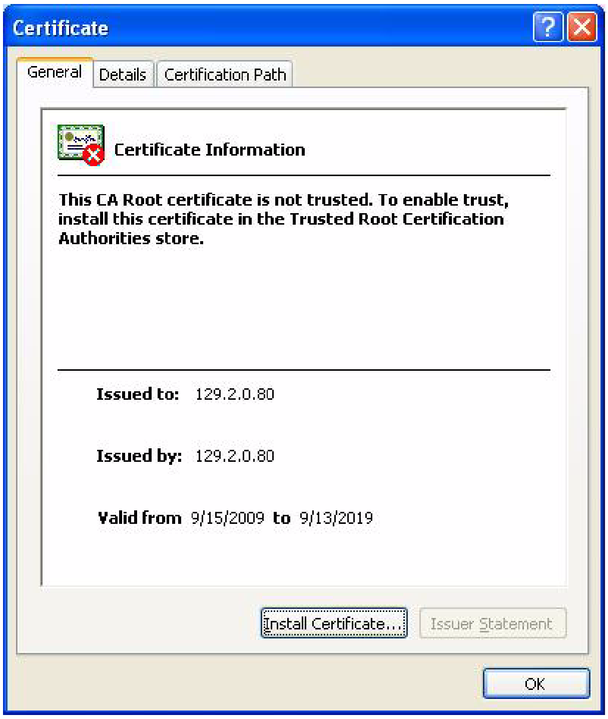
This problem may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage.

About certificate errors

View certificates

5. The screen below shows the certificate dialog.



Certificate Information

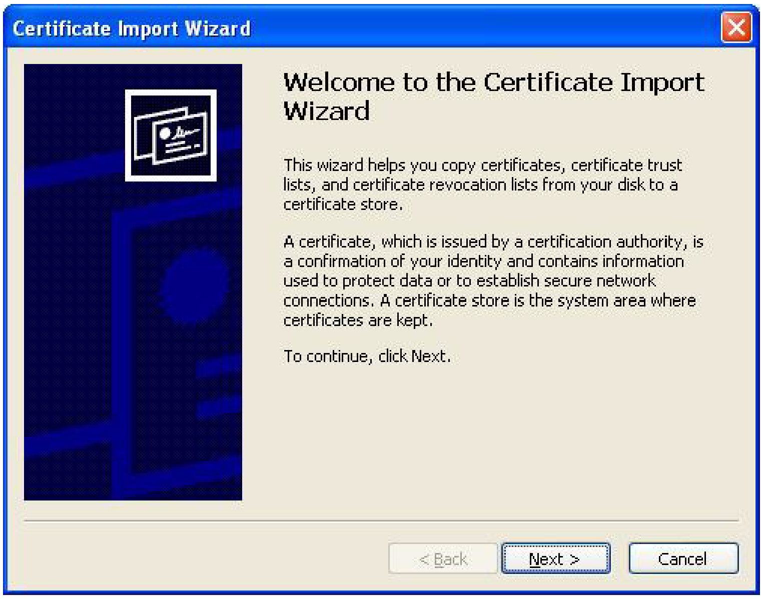
This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store.

Issued to: 129.2.0.80

Issued by: 129.2.0.80

Valid from 9/15/2009 to 9/13/2019

6. In the **General** tab, click **Install Certificates**. The screen below appears.



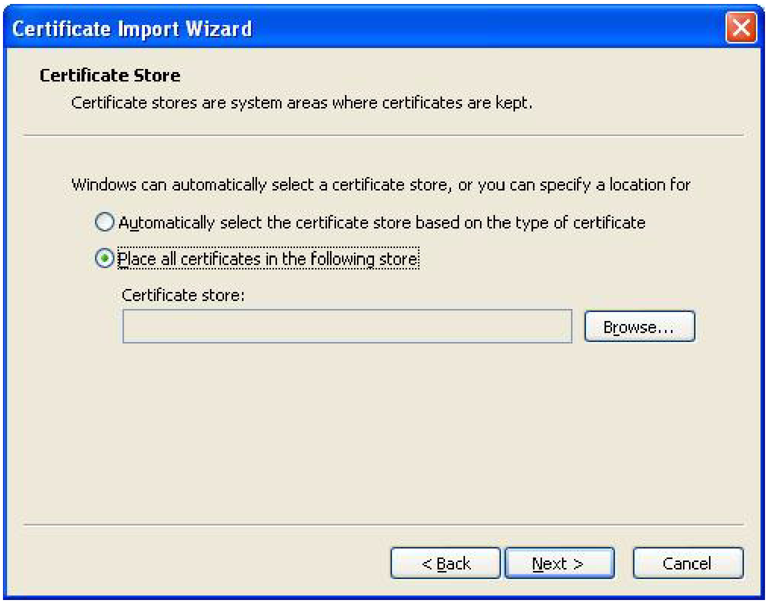
Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

7. Click the **Next** button to start importing the certificate.



Certificate Store

Certificate stores are system areas where certificates are kept.

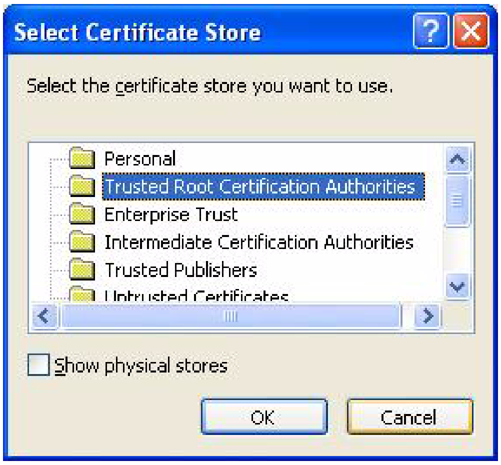
Windows can automatically select a certificate store, or you can specify a location for

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

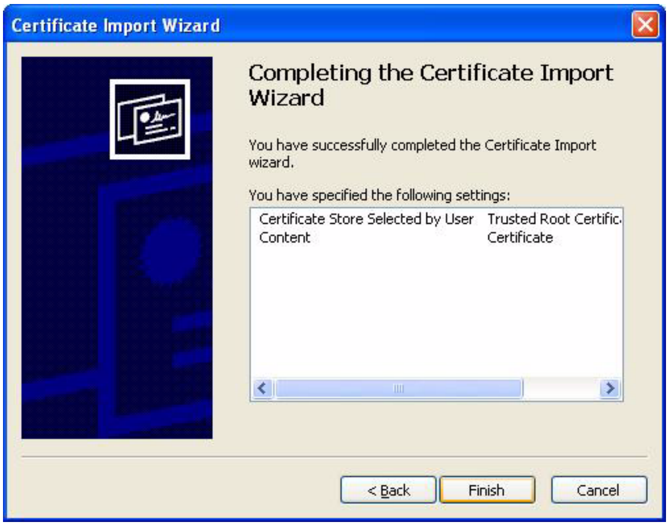
8. Select the radio button **Place all certificates in the following store**. Click the **Browse** button to select a location to save the certificates. The following window pops up for you to select the location.



Select the certificate store you want to use.

□ Show physical stores

9. Select the location **Trusted Root Certificate Authorities** and click the **OK** button.



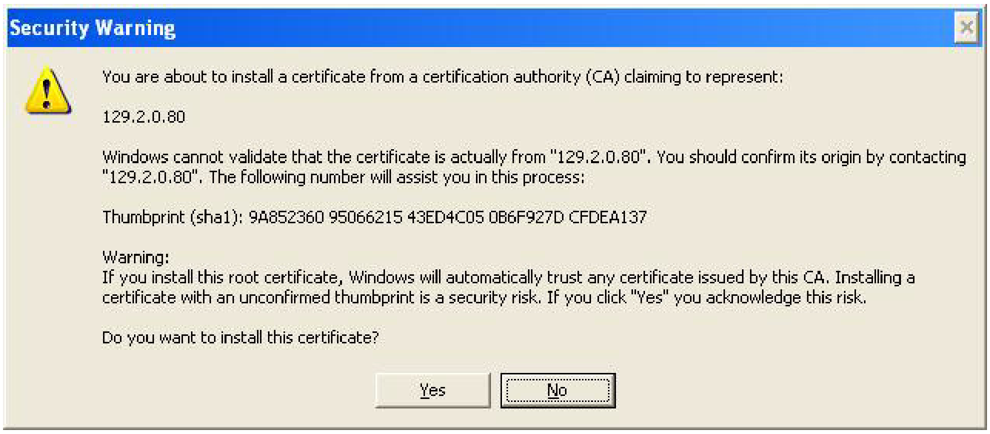
Completing the Certificate Import Wizard

You have successfully completed the Certificate Import wizard.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certific
Content	Certificate

10. Click the **Finish** button to complete the installation. The following security warning prompts.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

129.2.0.80

Windows cannot validate that the certificate is actually from "129.2.0.80". You should confirm its origin by contacting "129.2.0.80". The following number will assist you in this process:

Thumbprint (sha1): 9A852360 95066215 43ED4C05 0B6F927D CFDEA137

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

11. Click **Yes** to complete the installation. Enter the AEC2.1's IP address in the browser's Address box and the AEC2.1 login page appears without the certificate error message.

13.5 How to Set Initial Controller Configuration

Set the controller's IP address, subnet mask, and gateway address before installing the controller on the customer's network. Follow the instructions in this section to configure the controller.

1. Connect a computer running the Windows operating system directly to the AEC using the crossover network cable.
   - The computer that you use should be configured for the 192.168.0 network. We suggest the computer be configured for:
     IP address 192.168.0.40,
     Subnet mask 255.255.0.0
     Gateway .... 0.0.0.0.
   - Use the Crossover cable to connect the computer with the controller.

2. If not already done, power up the controller at this time.
   - The CPU board will perform a power-up self-test. This test takes about 90 seconds to complete. When the self-test is finished, TX and RX of the interface boards (4-Reader board and 8-IO board) should blink alternately.
   - Wait till the self-test is complete before proceeding.

NOTICE!
During the power-up self test duration, no communication with the controller is possible.

3. On the computer, open a Web browser application and enter the controller's IP address (192.168.0.41) in the browser's address or location bar. Then press the **Enter** key to connect to the controller.
   - If you have not used your browser to connect to AEC2.1 before, it may be necessary to make slight configuration changes within the browser setup to establish

   connectivity for the first time. The most common setup change needed is to instruct the browser to connect using a LAN rather than a dialup modem.
   - The controller should respond to the connection attempt by displaying the Login window.

4. Login to AEC2.1 using the user name “**user1**” and password “**8088**”. Select the required GUI language from the language dropdown. Click the Login button.
   Result: Upon successful login, the AEC2.1 home page is displayed.

5. From the home page, select **System** > **Network Settings**.
   Result: The Network Settings page displays.

6. Modify the Controller's IP Address, Subnet mask, and Gateway. Set these fields to the values provided by the customer.
   The values for these fields must be set correct for the controller to be able to operate over the customer's network. The required settings must be obtained from the customer, or a representative of the customer's Information Technology department.

   After changing the settings, click the 💾 save button to save the settings.

7. From the home page, select **System** > **Advance Configuration** > **System Maintenance** > **Reboot** to reboot the controller. This will cause the controller to reboot and load the new IP address information that was entered and saved in the previous steps.
   After rebooting, the controller will begin responding to its new address. It will no longer respond to the default address 198.168.0.41.

8. Before connecting the controller to the customer's network, it is advisable to test it using the new settings to confirm proper setup.
   - To do this, you will need to change the network configuration of your computer to an address on the same network as the controller.
   - As an example, assume that in the previous steps you set the controller's address to 192.9.200.18 and the Subnet mask to 255.255.0.0. To test the controller using your computer, the computer's network setup will need to be changed to a similar address on the same network. For example, you could set the computer to 192.9.200.19. You should set the netmask on the computer to the same value as the controller.
   - After changing network setup on the computer, the computer will need to be rebooted. After rebooting connect the AEC2.1 by entering the new controller address in the location or address bar of the browser.
   - If successful connection is made to the controller, the Login screen is displayed.

9. Once proper operation has been confirmed, Logout of the controller and close your browser. Then disconnect the crossover cable from both the controller and the computer.

The controller is now ready for connection to the customer's network. Usually, this connection is made to a wall jack or hub using a straight-through network cable.

14 Dial-In Networking

Introduction

The dial-in networking feature allows the controller administrator to remotely connect to the AEC2.1 for database management and/or monitoring purposes. After connecting, the AEC2.1 can be accessed through a browser.

General

The dial-in capability is implemented by connecting the AEC2.1's serial port to an external modem, and then connecting the modem to a dedicated analog telephone line. The controller's administrator can dial into the controller from any computer that supports dial-in networking.

Modem Guidelines

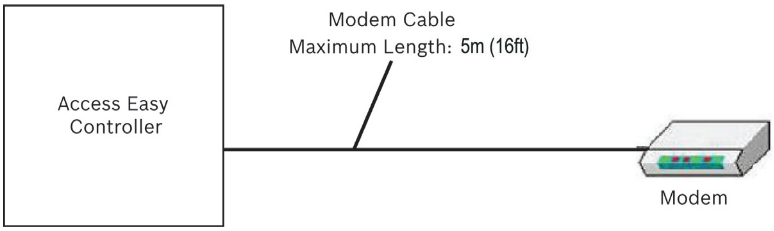
The AEC2.1 software has been designed to be as generic as possible in the implementation of modem support and dial-in networking. However, modems tend to have varying characteristics and attributes from one manufacturer to the other, and often from one model to the other within a given manufacturer.

For persons preferring to use a different modem, the set-up characteristics needed by the modem are documented later in this chapter. Understand that when using a non-standard modem, Bosch Security Systems and supplier support services will not be able to provide troubleshooting and technical support for modem-related issues.

14.1 Guidelines for Modem Installation - Not Investigated by UL

The modem must be installed in the same room as the controller.

The cable length between the modem and the RS-232 port on the AEC2.1 must not exceed 5m (16ft) in length.



Note: UL listed and/or recognized wire must be used for cabling and wire suitable for the application.

14.2 Installing the Modem

1. Connect the modem to the AEC2.1's serial port using the cable provided with the modem. If this is a UL-compliant installation, be sure to adhere to the guidelines in the previous section.

2. The diagrams below indicate the location of the controller's serial port that is connected to the modem.

NOTICE!

AEC2.1 only supports US Robotics dial-in Modems. For other brands of modem, refer to dial-in protocol section to check modem compatibility.

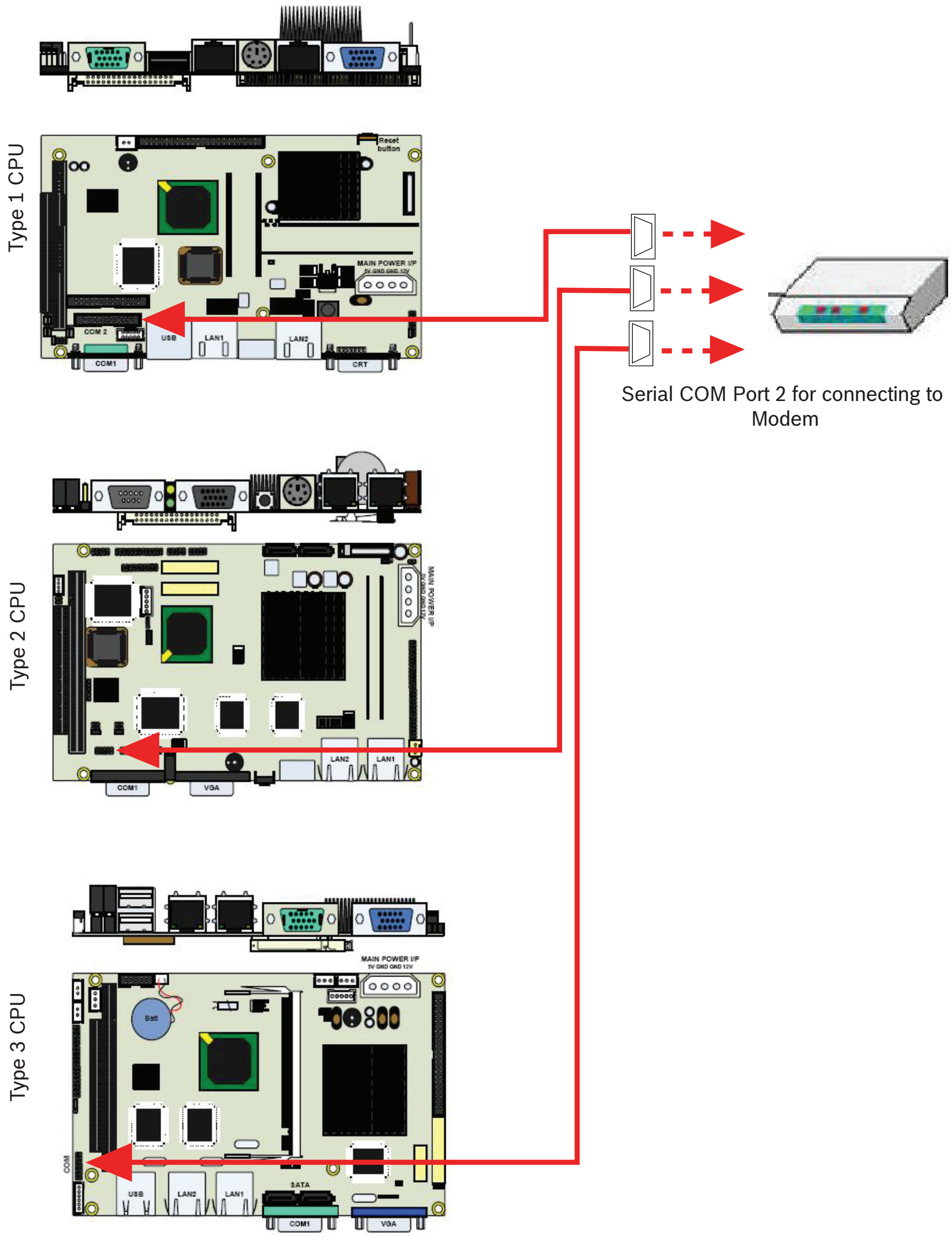


Figure 14.1 Serial COM port 2 of CPU's used to connect to a modem

3. Connect cable from the 9-volt transformer supplied with the modem into the connector on the back of the modem. Leave the modem powered off at this time.

4. Connect one end of the telephone cable provided with the modem to the wall jack and the other end into the connector on the back of the modem. There are two connectors on the back of the modem. Be sure to connect the cable to the incoming phone line

connector. This connector may be labelled “incoming line” or there may be a drawing of a phone jack to indicate the proper connector.

5. Depending on the model of the modem, some has switches on the back or the side, the table below acts as a guide for the type of settings that is needed. Refer to the modem manual for more information.

14.2.1 Modem Switch Settings

Switch	Setting	Function
1	OFF	Data Terminal Ready (DTR) Override – OFF - Normal DTR operations: computer must provide DTR signal for the modem to accept comment; dropping DTR terminates a call – ON - Modem ignores DTR (Override)
2	OFF	Verbal/Numeric Result Codes – OFF - Verbal (word) results – ON - Numeric results
3	ON	Result Code Display – OFF - Suppresses result codes – ON - Enables result codes
4	OFF	Command Mode Echo Suppression – OFF - Displays keyboard commands – ON - Suppresses echo
5	OFF	Auto-Answer Suppression – OFF - Modem answers on first ring, or higher if specified in NVRAM – ON - Disable auto-answer
6	OFF	Carrier Detect (CD) Override – OFF- Modem sends CD signal when it connects with another modem, drops CD on disconnect – ON - CD always ON (Override)
7	OFF	Power-on and ATZ Reset Software Defaults – OFF - Loads Y0-Y4 configuration from user-defined non-volatile memory (NVRAM) – ON - Loads & FO - Generic template from read-only memory (ROM)
8	ON	AT Command Set Recognition – OFF - Disables command recognition (Dumb Mode) – ON - Enables recognition (Smart Mode)

6. Power up the modem using the off/on switch located on the front. The AA, TR, and CS indicators should light. All others should be off.

NOTICE!
The next step of this procedure requires that the AEC2.1 be reset. If the controller is currently in use, then you may want to back up the controller's database before continuing.

7. Reset the AEC2.1 and wait for the controller to complete its initialisation process. This typically takes about 90 seconds.

   Immediately upon the completion of the initialisation process, the controller senses the presence of the modem and sends it a serial of initialisation commands. By carefully watching the lights on the front of the modem, you can see the command transfer taking place. The SD and RD indicators will flash faintly for a couple of seconds as the initialisation commands are sent to the modem. The final command in the series instructs the modem to save the current setup. The commands sent to the modem by the controller are listed below.

   attTone mode

   atzReset

   ate0Echo Off

   ats0=1One ring to autoanswer

   atb0Selects the ITU-T V.25 answer sequence

   at&b1Fixed DTE speed (serial port rate)

   at&wSave settings

8. Test the modem and modem-to-controller wiring by dialling the phone number to which the modem is connected from any standard telephone. The modem should answer on the first ring and you should hear the usual tones indicating that the modem is attempting to synchronize with the calling party. If modem tones are heard, then this test is successful and you can hang up the phone.

9. This completes the modem installation. Proceed below to configure the security features associated with AEC2.1 dial-in networking.

14.3 Dial-in Security Features

The AEC2.1 includes some additional security features to provide protection against unauthorized access to the controller over the dial-in connection. These include the following:

First, a special login ID and password is used to establish the dial-in session. Once the session has been established, then a second login is required, using a regular user id and password, to gain access to the controller. The special login id and password, which are used only with dial-in networking, is user configured.

Second, there is a parameter that specifies the maximum number of unsuccessful login attempts that will be allowed. When this value is reached without a successful dial-in login, the controller will automatically disable the dial-in capability for a user-specified period of time.

The default settings for the security features are:

User ID - PPP
Password - 8088
Number of illegal password attempts - Undefined
Illegal attempts lockout duration - 0 minutes

All the dial-in security parameters are user-configured. However, it is suggested that they remain at the default settings until the installation is complete and the dial-in connection is fully operational.

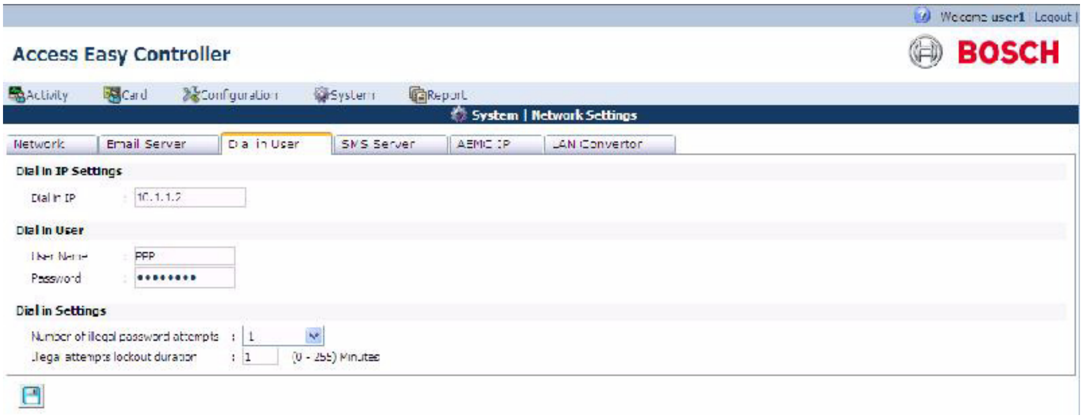
Follow the directions below to change the dial-in security settings.

14.4 Controller Setup

Dial-in networking allows you to remotely connect to the AEC2.1 through a phone line. Follow the steps below to configure dial-in networking.

1. Log into AEC2.1 and from the main page select **System** > **Network Settings**.

2. Select **Dial-In** tab and the screen below appears:



Dial In IP Settings
Dial In IP : 10.1.1.2

Dial In User
User Name : PPP
Password : ••••••••

Dial in Settings
Number of illegal password attempts : 1
Illegal attempts lockout duration : 1 (0 - 255) Minutes

3. The default Dial-in user name is 'PPP' and the default password is '8088'. For security purposes, change the default User Name and Password.

4. Adjust the Dial-in setting as necessary. Click the save button to save the settings.

14.5 Handling of IP Addresses by Access Easy Controller 2.1

When dial-in networking is used to connect to the AEC2.1, the connection is made using a communication point-to-point protocol (PPP). The PPP is used whenever a computer establishes a dial-in connection to any server. In the case of AEC2.1, the controller acts as the server and establishes the PPP connection to the customer's computer.

When a dial-in session is started, the server assigns an IP address to the computer that has dialed-in and requested the session. In this case, the server is the AEC2.1. The IP address that is assigned to the computer making the dial-in request is obtained from a database parameter in AEC2.1, which can be managed as necessary from the System section of the database.

Normally, the dial-in IP address is managed automatically by AEC2.1 based on the network address that is assigned to the controller during the installation and setup process. If the controller is assigned a Class A network address, then the controller will automatically configure the dial-in IP address to a Class C address. If the controller is assigned a Class B or Class C network address, then dial-in networking will automatically be configured to a Class A address. In most cases, the different class of the dial-in IP address will prevent any conflict or duplication of IP addresses within the customer's network.

14.6 Changing the Dial-In IP Address

Normally, the dial-in IP address is managed automatically by the controller and need not be changed. A possibility exists, however, that the automatically assigned dial-in IP address could conflict with another computer on the customer's network. In that case, it will be necessary to modify the default dial-in IP address.

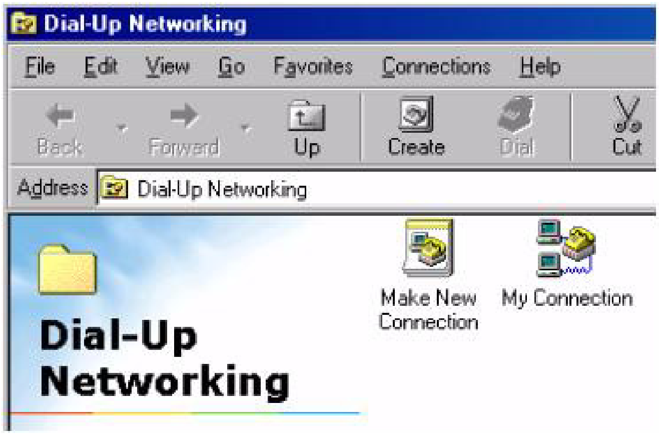
To change the dial-in IP address, connect to the AEC2.1 over the network and login. Select

System > **Network Settings** > **Dial-In** tab. Modify the IP address and click the 💾 save button to save the settings.

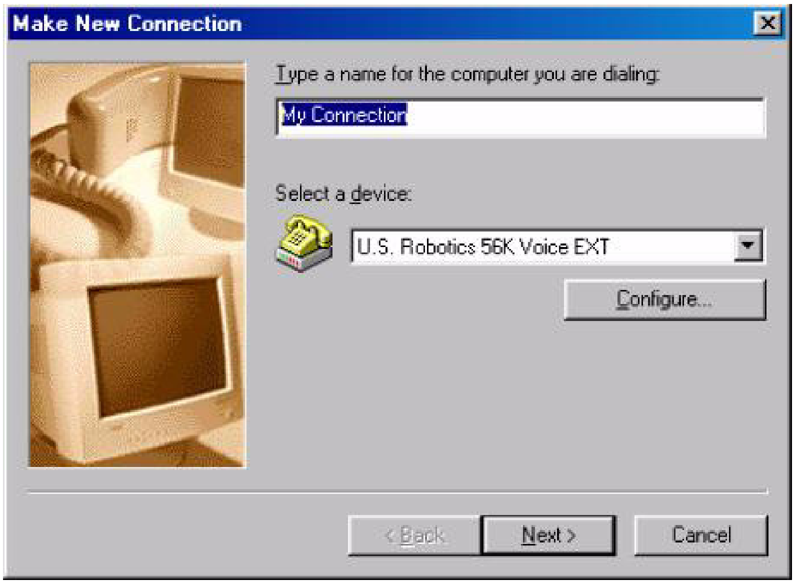
14.7 Configuring a Windows Computer to Dial the Access Easy Controller 2.1

To dial-in to an AEC2.1 from a computer, you must create a connection in Dial-in Networking.

1. On the computer that will be dialling into the AEC2.1, select **Start** > **Programs** > **Accessories** > **Communications** > **Dial-in Networking**. The screen below appears:



2. Double-click **Make New Connection** and the screen below appears. Enter a name for the connection (e.g., Access Easy Controller HQ)

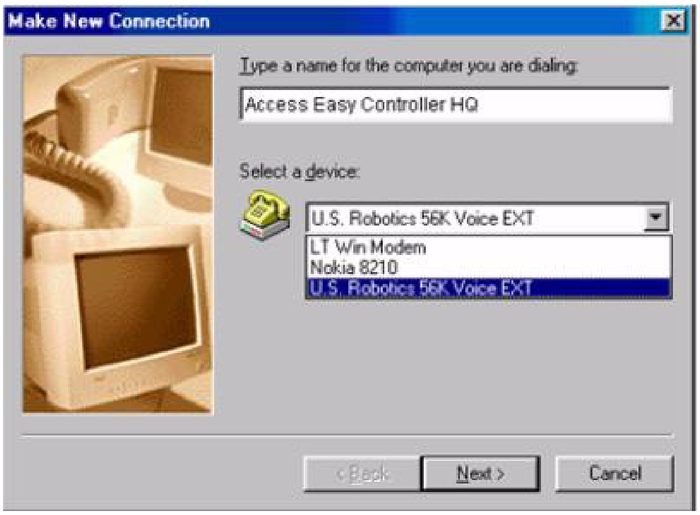


Make New Connection

Type a name for the computer you are dialing: My Connection

Select a device: U.S. Robotics 56K Voice EXT

3. Follow all on-screen instructions. Make sure a modem is connected to your computer. Select the appropriate modem from **Select a device** dropdown list as shown in the figure below.



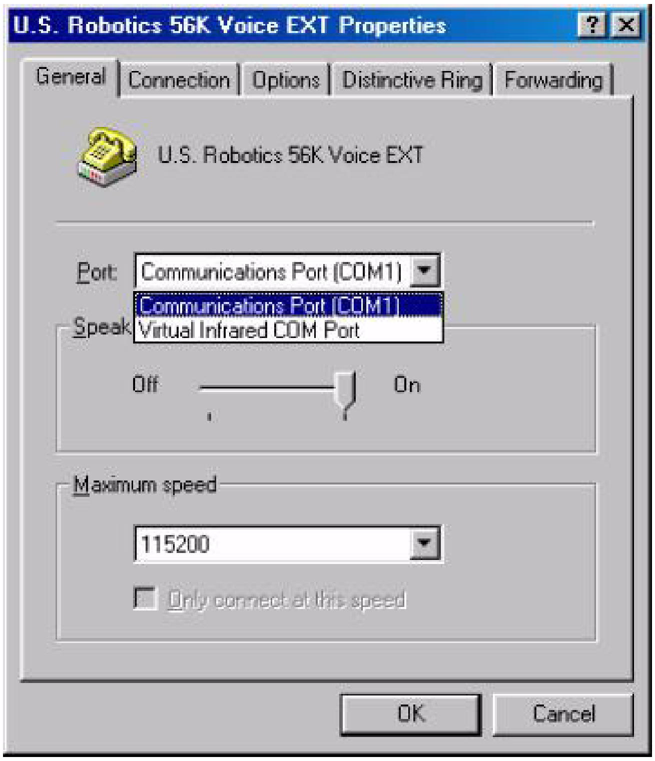
Make New Connection

Type a name for the computer you are dialing: Access Easy Controller HQ

Select a device: U.S. Robotics 56K Voice EXT

4. Click the **Next** button.

5. Configure your modem by selecting the **General** tab and setting available option, as appropriate. Select the **communications** port and accept the maximum speed default setting.


U.S. Robotics 56K Voice EXT Properties

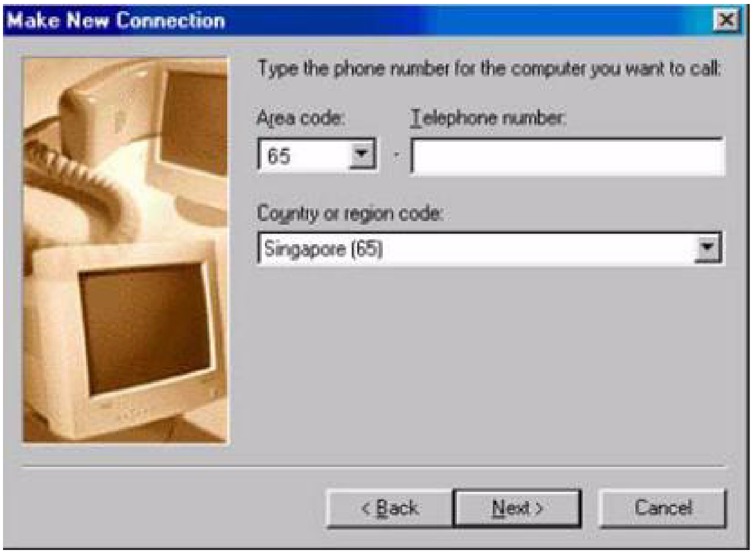
U.S. Robotics 56K Voice EXT

Port: Communications Port (COM1)

Maximum speed: 115200

□ Only connect at this speed

6. After configuring your modem, click the OK button and continue with the Make New Connection dialog box as shown below. Enter the controller's area code and phone number. Select your country or region code.


Make New Connection

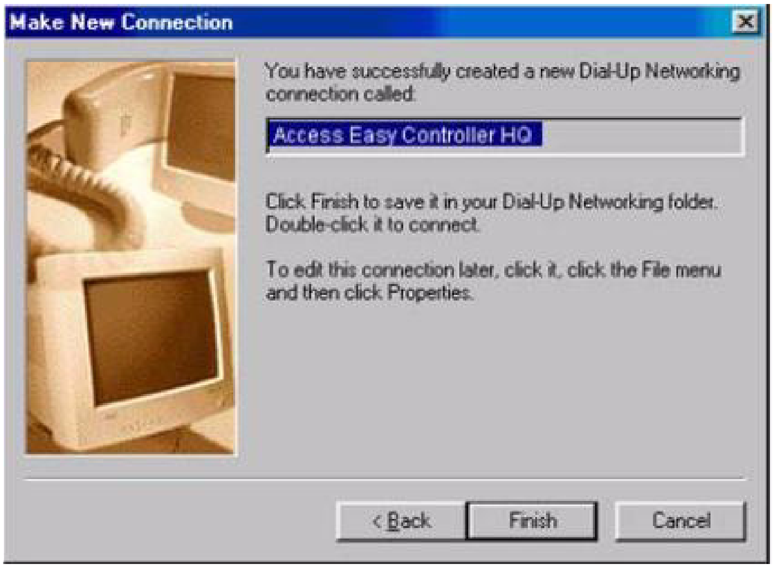
Type the phone number for the computer you want to call:

Area code: 65

Telephone number:

Country or region code: Singapore (65)

7. Enter the telephone number for AEC2.1 to which you want to connect, click the **Next** button, and the below screen appears.


Make New Connection

You have successfully created a new Dial-Up Networking connection called:

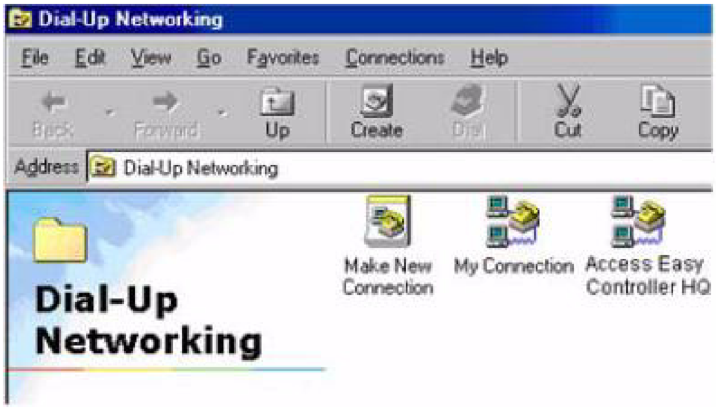
Access Easy Controller HQ

Click Finish to save it in your Dial-Up Networking folder. Double-click it to connect.

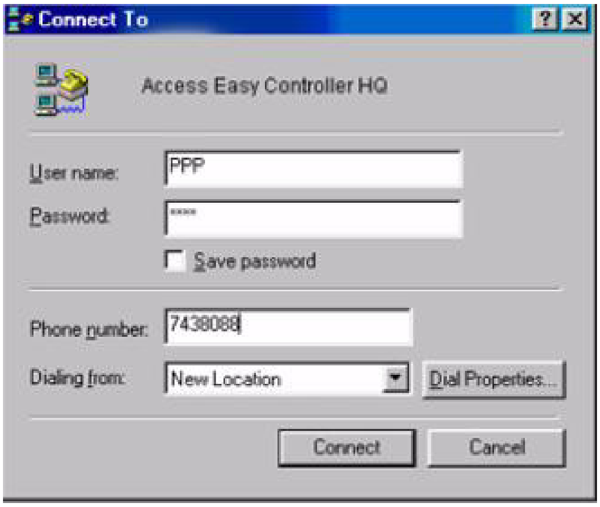
To edit this connection later, click it, click the File menu and then click Properties.

8. Click the **Finish** button.

9. Return to Dial-in Networking as explained in step 1 to view your new connection.



10. To connect to the AEC2.1, double-click the Access Easy Controller HQ icon, the screen below appears.


Connect To

Access Easy Controller HQ

User name: PPP

Password: ****

□ Save password

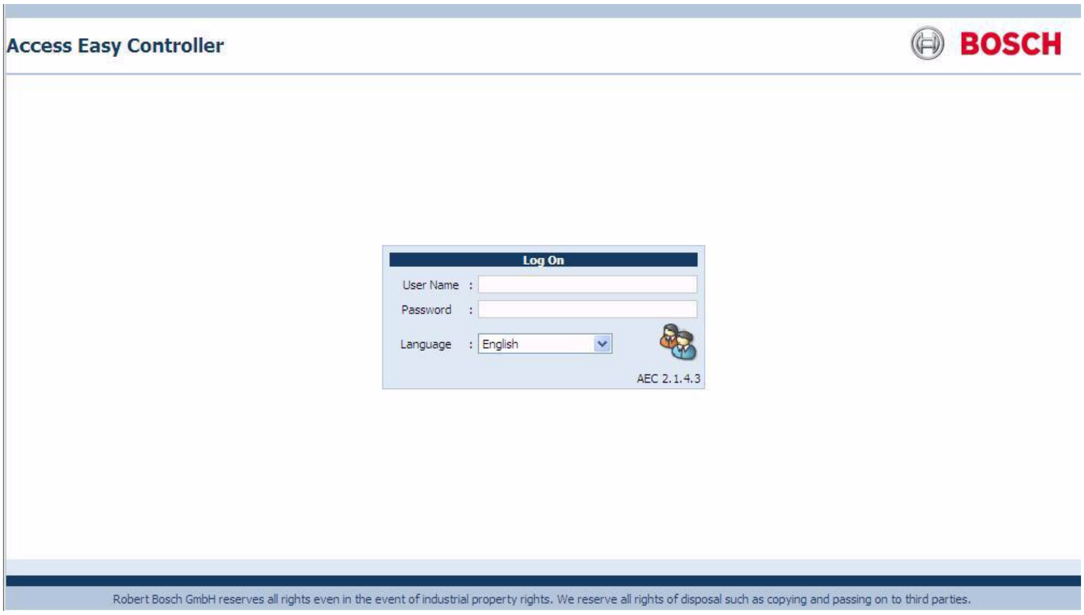
Phone number: 7438088

Dialing from: New Location

11. In the **User name** and **Password** boxes, enter the Dial-In User name and password of the AEC2.1 to which you want to connect. Then, if it is not already displayed, enter the appropriate phone number and click the Connect button.

NOTICE!
It will take about 30 seconds from the time the controller's modem answers the incoming call till the user id and password are validated and the dial-in user is registered by the controller. Most versions of dial-in networking will display a message to the user when the dial-in authentication process is completed. Wait for the connection to complete before proceeding to the next step.

12. After successfully connecting, open your Web browser. Type the IP address of the AEC2.1 in the address bar of the browser and press the **Enter** key. If you have successfully connected to the controller, the AEC2.1 Login screen appears.



Language : English

Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

13. Log in to the controller by entering a valid user id and password and click the Login button.

14.8 Handling Simultaneous Network and Dial-in Connections

In the unusual case where you may attempt to connect to AEC2.1 over a dial-in connection from a computer that is on the same local area network as the controller, there is a possibility that Internet Explorer may not be able to establish the dial-in connection with the controller. There is a setting on the computer that can be changed to force the browser to use the dial-in connection.

In the Windows operating system, go to Settings > Control Panel and select Internet Options. Click the Connections tab and make sure the option Always dial my default connection is selected.

15 Restoring a Backup Copy of Database to the Access Easy Controller 2.1

This chapter explains the necessary steps to restore a copy of the controller's database from a backup stored on the computer. This chapter helps recover the customer's database without the necessity of complete re-entry. It would be used only under the following circumstances:

- The controller's CPU board has been replaced due to a hardware failure.
- To install a software upgrade in an operational controller

In both instances, it is desirable to reinstall the customers' existing database, rather than re-entering the complete database.

15.1 Tools Needed

- Computer with network card and Windows operating system
- Connectivity between the computer containing the database and the controller through the network or directly by use of a crossover cable

15.2 Before Starting the Update

1. Log on to the controller.

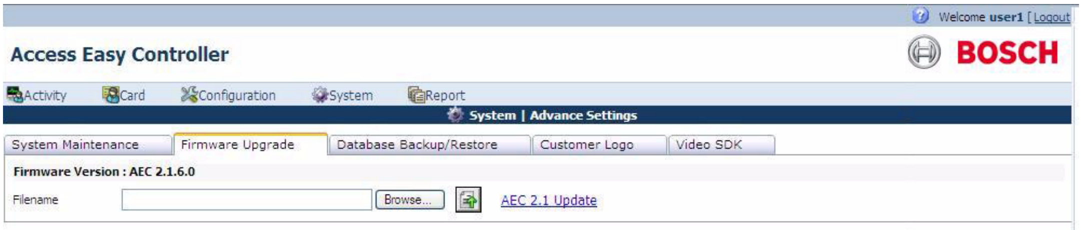
2. After logging on, select **System** > **Network Settings** and note the IP addresses and Remote PC addresses and hostnames listed under the section heading Remote PC Addresses. For security reasons, only a computer with an IP address matching one of the three shown in this section will be allowed to make the FTP connection necessary to recover the controller database.

3. If the IP address of the computer to be used for database recovery does not match one of the three listings shown in the database, then the connection will be denied. In that case, it is necessary to change the settings of either the computer or the controller's database so that they match. This should be done before proceeding to the recovery procedure. If the controller database is changed, save the changes before proceeding.

15.3 Recovering Controller Database from a Windows Computer

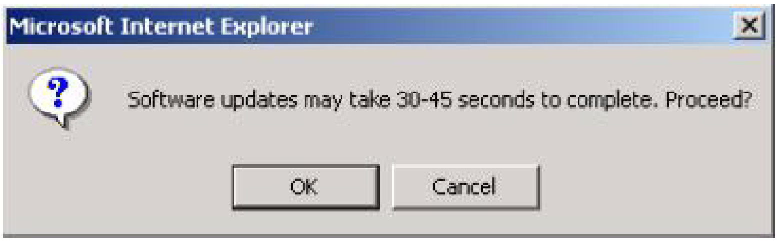
1. Log into AEC2.1 and select **System** > **Advance Settings** > **Firmware upgrade** tab.

2. Click the browse button to browse for the file you wish to upload. Example, if you are uploading the backup system database, select the db_tar.gz from your local directory



Firmware Version : AEC 2.1.6.0

3. Click the upload button to upload the file. The dialog box below appears for confirmation



Software updates may take 30-45 seconds to complete. Proceed?

4. Click the OK button to proceed.

   Once the process is completed without error a successful message is displayed.

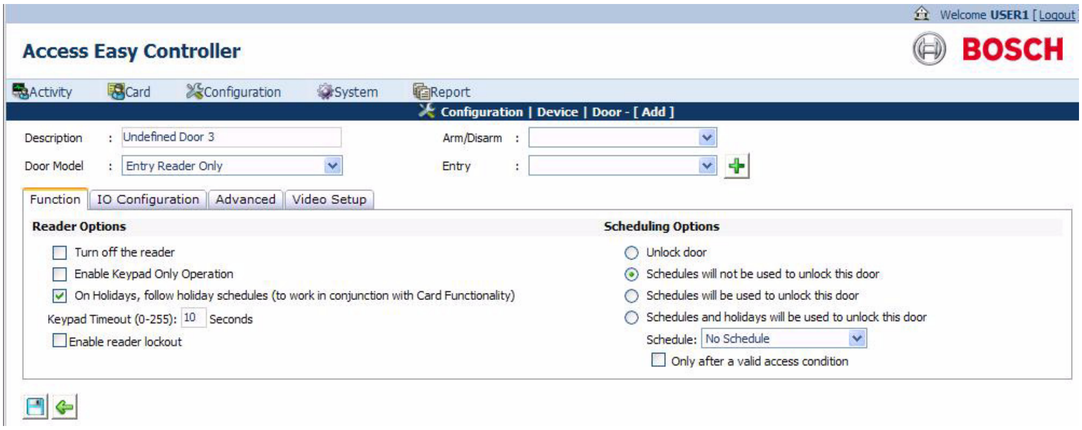
5. Click the OK button and reboot the AEC2.1.

16 Entry and Arm/Disarm Reader

AEC2.1 has the option to configure a reader as a normal door access reader and acts as an Arming/Disarming reader at the same time. In order to achieve dual operation on the reader, there are certain settings required.

The reader should be first configured as an Entry reader and must be set to an alarm zone to arm/disarm the reader. Follow the steps below to set the reader as Entry and Arm/Disarm reader:

1. In the AEC2.1 software setup, select **Configuration** > **Device** > **Door** and click the ✚ button to add new door settings. The screen below appears.



Configuration | Device | Door - [Add]

Description : Undefined Door 3

Door Model : Entry Reader Only

Arm/Disarm :

Entry : ✚

Reader Options

- ☐ Turn off the reader
- ☐ Enable Keypad Only Operation
- ☑ On Holidays, follow holiday schedules (to work in conjunction with Card Functionality)
- Keypad Timeout (0-255): 10 Seconds
- ☐ Enable reader lockout

Scheduling Options

- ○ Unlock door
- ● Schedules will not be used to unlock this door
- ○ Schedules will be used to unlock this door
- ○ Schedules and holidays will be used to unlock this door
- Schedule: No Schedule
- ☐ Only after a valid access condition

2. Enter a description for the reader in the **Description** field.

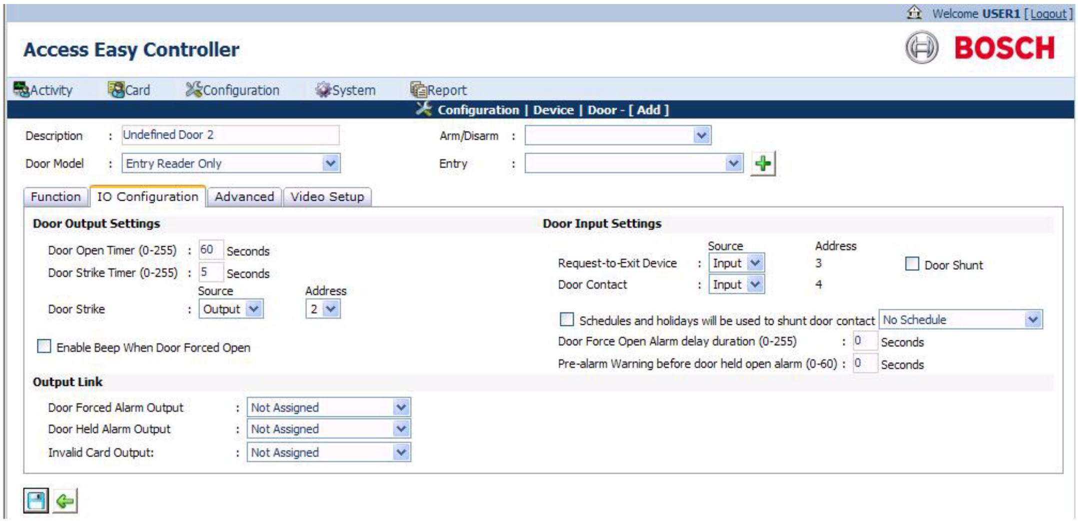
3. Select **Entry Reader Only** from the **Door Model** dropdown list.

4. Select an **Alarm zone** from the **Arm/Disarm** dropdown list, this will be the zone that the reader will arm and disarm

5. Select the Reader from the **Entry Reader** dropdown list.

6. Click the 💾 save button to save the setting.

7. Click the **IO Configuration** tab to configure the IOs of the reader. The screen below shows the IO Configuration page.



Description : Undefined Door 2

Door Model : Entry Reader Only

Arm/Disarm :

Entry :

Door Output Settings

Door Open Timer (0-255) : 60 Seconds

Door Strike Timer (0-255) : 5 Seconds

Door Strike : Source: Output Address: 2

□ Enable Beep When Door Forced Open

Output Link

Door Forced Alarm Output : Not Assigned

Door Held Alarm Output : Not Assigned

Invalid Card Output: : Not Assigned

Door Input Settings

Request-to-Exit Device : Source: Input Address: 3 □ Door Shunt

Door Contact : Source: Input Address: 4

□ Schedules and holidays will be used to shunt door contact No Schedule

Door Force Open Alarm delay duration (0-255) : 0 Seconds

Pre-alarm Warning before door held open alarm (0-60) : 0 Seconds

8. At this point you should configure all the settings related to the door access, such as **Door Strike Timer**, **Door Open Timer**, **Door Strike**, etc

NOTICE!
There is an additional setting available which is the Door Buzzer. When a reader is configured as an **Entry and Arm/Disarm** reader, the buzzer control for the reader will need to be rewired to a spare output on the 4-Reader board. See the wiring diagram below for an example on Reader1 wired as an Entry and Arm/Disarm reader.

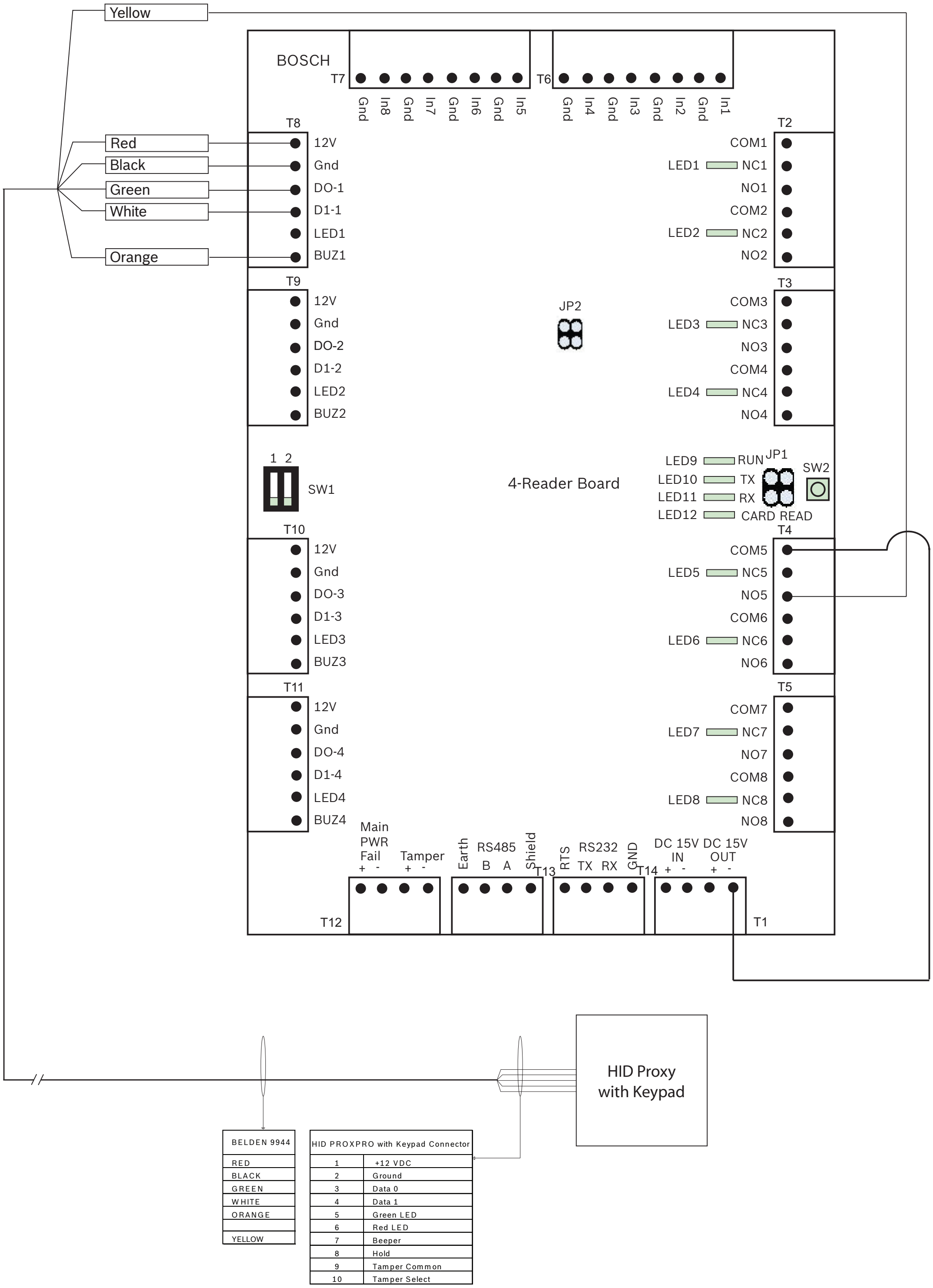
9. Complete the rest of the setup as per a normal door access reader.

10. You need to configure the cardholder to be able to arm/disarm the reader. Refer to AEC2.1 software manual for configuring an Arm/Disarm card.

11. The section below shows the wiring requirement of Entry and Arm/Disarm Reader for a HID reader.

NOTICE!
Refer the software manual for more information on the door settings.

16.1 Wiring diagram of a HID Compliant Entry and Arm/Disarm Reader



BELDEN 9944
RED
BLACK
GREEN
WHITE
ORANGE
YELLOW

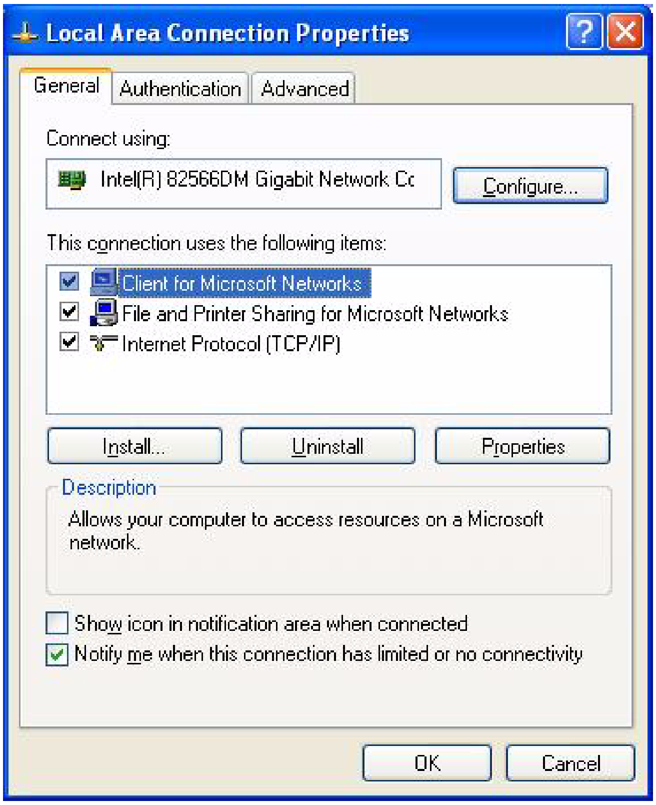
HID PROXPRO with Keypad Connector	
1	+12 VDC
2	Ground
3	Data 0
4	Data 1
5	Green LED
6	Red LED
7	Beeper
8	Hold
9	Tamper Common
10	Tamper Select

17 Appendix A How to Install & Set the TCP/IP Address on a PC

This chapter describes the steps required to install TCP/IP communication protocol on a computer and to assign an IP address to a computer.

1. Click the start button, followed by **Setting** > **Control Panel** > **Network Connections**.

2. Double-click the existing network connection icon and select **Properties**, the screen below appears.



Local Area Connection Properties

Connect using:

Intel(R) 82566DM Gigabit Network Cc

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

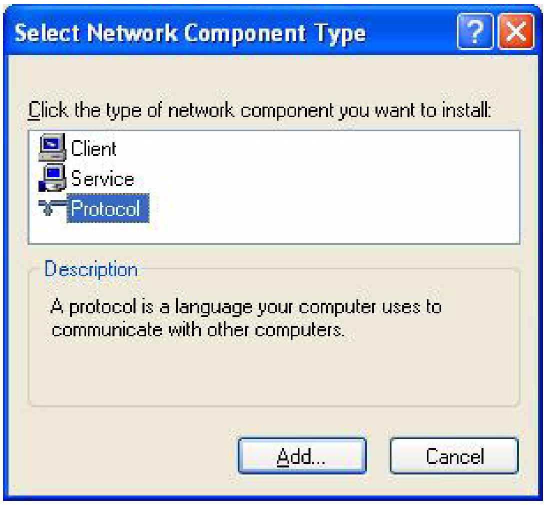
Description

Allows your computer to access resources on a Microsoft network.

- □ Show icon in notification area when connected
- ☑ Notify me when this connection has limited or no connectivity

3. Look up for **Internet Protocol TCP/IP** from the list. If the component is found, highlight it by single clicking on it. Then skip forward to step 8 of this procedure. However if the component is not found, continue with steps 4 to 7 and install the component.

4. If Internet Protocol TCP/IP is not found, then you need to install it. To add the TCP/IP component, click the Install... button, the screen below appears:

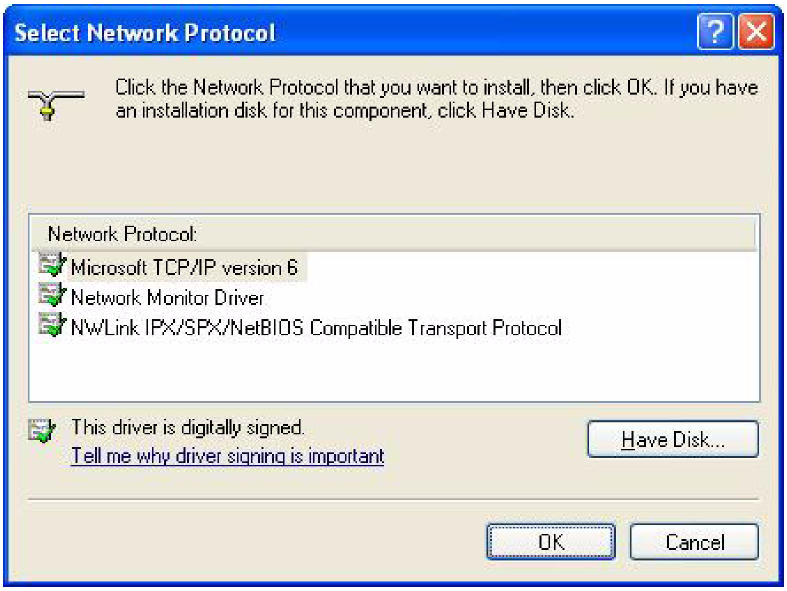


Click the type of network component you want to install:

A protocol is a language your computer uses to communicate with other computers.

5. Highlight the Protocol line by single clicking on it, and then click the Add... button.

6. The dialog box below appears. From this box, select **Microsoft TCP/IP version 6** in the Network Protocol window.

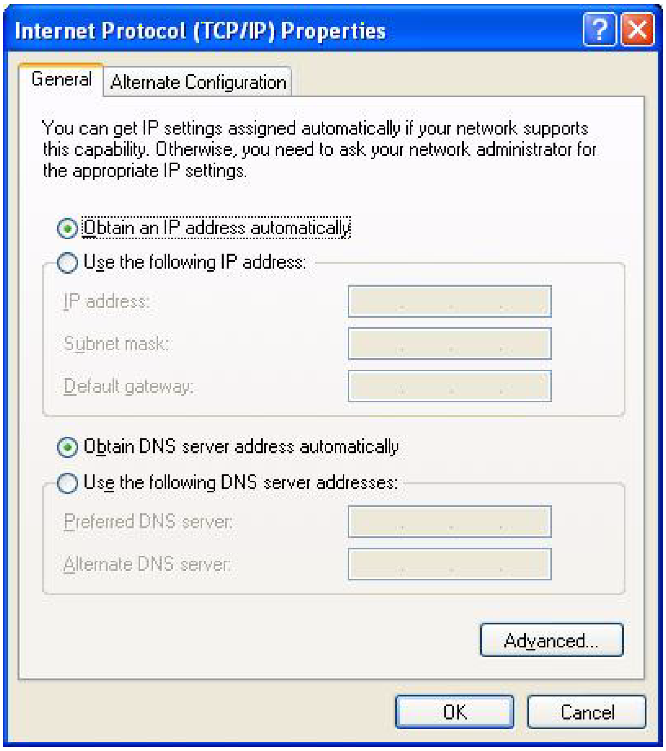

Select Network Protocol
?
Network Protocol:
Microsoft TCP/IP version 6
Network Monitor Driver
NWLink IPX/SPX/NetBIOS Compatible Transport Protocol
Tell me why driver signing is important
Have Disk...
OK
Cancel

Click the Network Protocol that you want to install, then click OK. If you have an installation disk for this component, click Have Disk.

This driver is digitally signed.

7. Click OK to proceed with the component installation. Follow any instructions that may be displayed on the screen. Note that the system may ask you to insert your Windows Installation Disk in the CD ROM drive. When done, go back to step 3 and select the TCP/IP Protocol - network adapter line from the list of installed network components. Then proceed to step. 8.

8. With the TCP/IP - adapter component highlighted, click the Properties button to define the TCP/IP Properties. The TCP/IP properties dialog box appears as shown below



Internet Protocol (TCP/IP) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

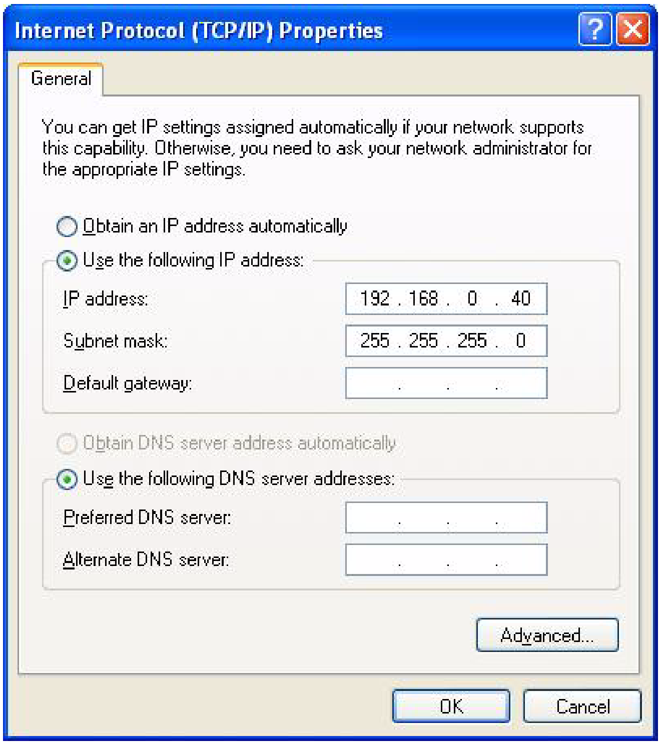
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

9. Select Use the following IP address radio button. This will enable the fields for IP Address and Subnet Mask.

10. Enter the IP Address and Subnet Mask Address. The following examples shows the recommended address and subnet mask to assign to the computer to communicate with a brand new AEC2.1 as received from the factory. Leave DNS field blank



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 40

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

11. Click the OK button after verifying the IP address and subnet mask.

12. The computer will proceed to configure the TCP/IP settings. When completed, you will be prompted to reboot the computer for the new settings to take effect.

18 Appendix B Modem Setup

18.1 Preparing the WAVECOM GSM Modem for AEC2.1

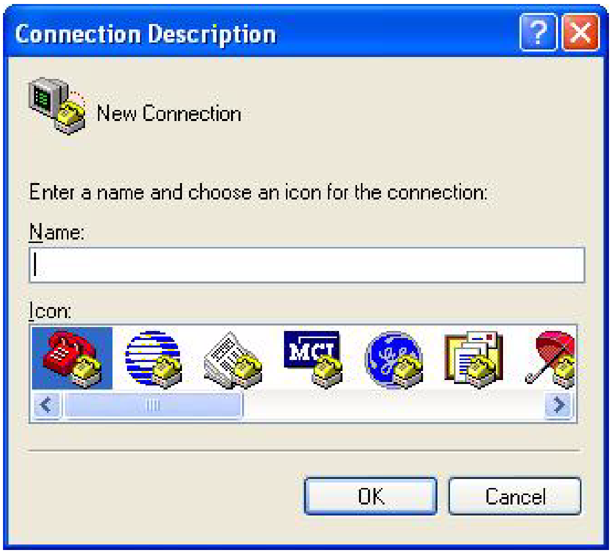
1. Insert the SIM Chip into the GSM Modem.

2. Power up the GSM modem

3. Connect the PC serial port, and the Modem using the serial cable that comes with the Modem.

4. Go to **Start** > **Programs** > **Accessories** > **Communication** > **HyperTerminal**.

5. You will be prompted to enter the name of the connection, enter any name in the **Name** field.



Connection Description

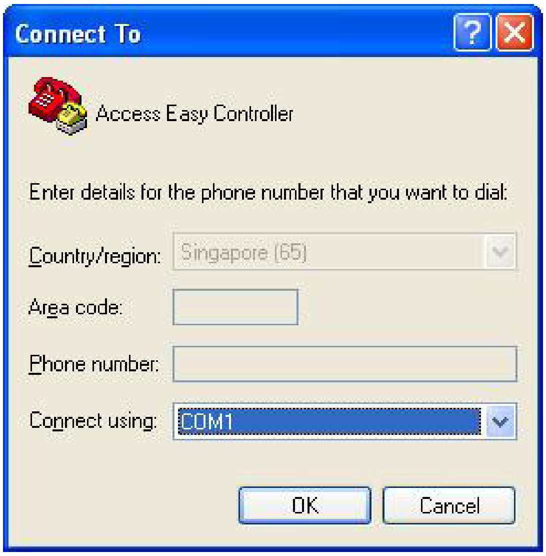
New Connection

Enter a name and choose an icon for the connection:

Name:

Icon:

6. Select the comport that the GSM Modem is connected to



Connect To

Access Easy Controller

Enter details for the phone number that you want to dial:

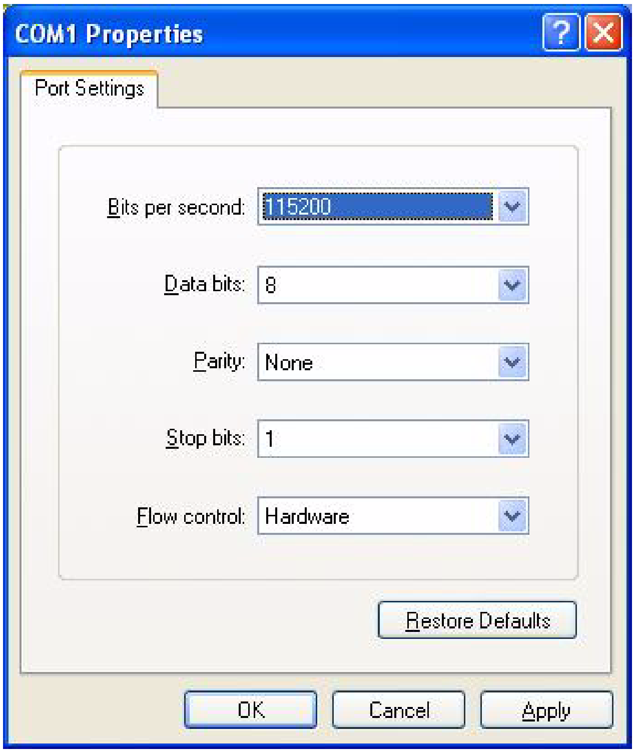
Country/region: Singapore (65)

Area code:

Phone number:

Connect using: COM1

7. Click the OK button and in the next screen set the **Baud rate**, set it to **115200** Bits per second, **8** Data bits, **1** stop bit and **None** in the Parity as shown below.



COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: Hardware

8. Click the OK button to start the connection.

NOTICE!
Once connected, you should check whether the connection is stable by typing “**AT**” followed by **enter**, you should get an “OK” reply from the GMS modem.
If there is no reply or the reply is not “**OK**” but display some unknown character, then it is possible that the GSM Modem baud rate is incorrect. Change the baud rate and reconnect.

9. Once you have connected to the GSM Modem, don’t change the baud rate.

10. Type “AT+IPR=19200” and press the **enter** key. You should get an “OK” replay.

11. Now you will need to change your baud rate of the **HyperTerminal** to **19200**.

12. Click the disconnect icon to disconnect the connection.

13. Click the change icon to change the Baud rate to 19200 and then click the connect icon to reconnect with the GSM modem again.

14. Type “AT” followed by a return, if the GSM modem replies “OK” then the configuration is complete.

15. You will need to save the configuration into the non -volatile memory in the GSM modem.

16. Type “AT&W” followed by a return, the GSM modem will reply “OK”.

17. Reboot the GSM modem and try connecting again to the GSM modem using the baud rate 19200.

18.2 How to Test the GSM Modem

You could test whether the GSM modem is working before connecting it to the AEC2.1.

1. Firstly set the GSM Modem as shown above, and then connect the GSM Modem to the PC via the serial port and run HyperTerminal. Follow the steps below to send out a test sms.
   Type “AT+CMGS=xxxxxxxx” followed by a return, you will expect to see a “>” reply from the GSM Modem. (xxxxxxxxx denote the mobile number)

2. Next type the message “TESTING TESTING” followed by <ctrl-Z> followed by a return, you will expect to see a “+CMGS: nn” followed by a “OK”, this means the sms is sent successfully. (nn denote a double digit number provided by the GSM modem).

NOTICE!
Model supported by AEC2.1

– Wavecom Fastrack Supreme 10 (Quad Band External GSM Modem)

19 Appendix C Detailed Wiring

This appendix shows the detailed wiring diagram of the Main Controller Unit for the system. The type of cable specification is tabulated below the image for quick reference.

NOTICE!

- The image for the Main Controller only shows the general connection between itself and other boards. Based on UL requirement, 2 different kinds of CPU board can be deployed, however, only one type will be used in each Main Controller.
- Wiring methods shall be in accordance with the National Electrical Code (ANSI/NFPA70), local codes, and the authorities having jurisdiction

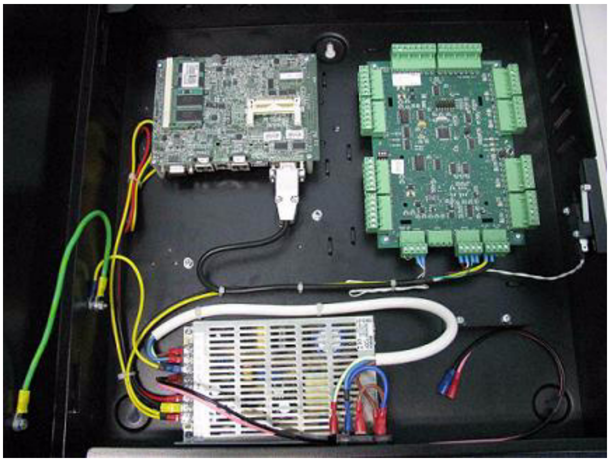


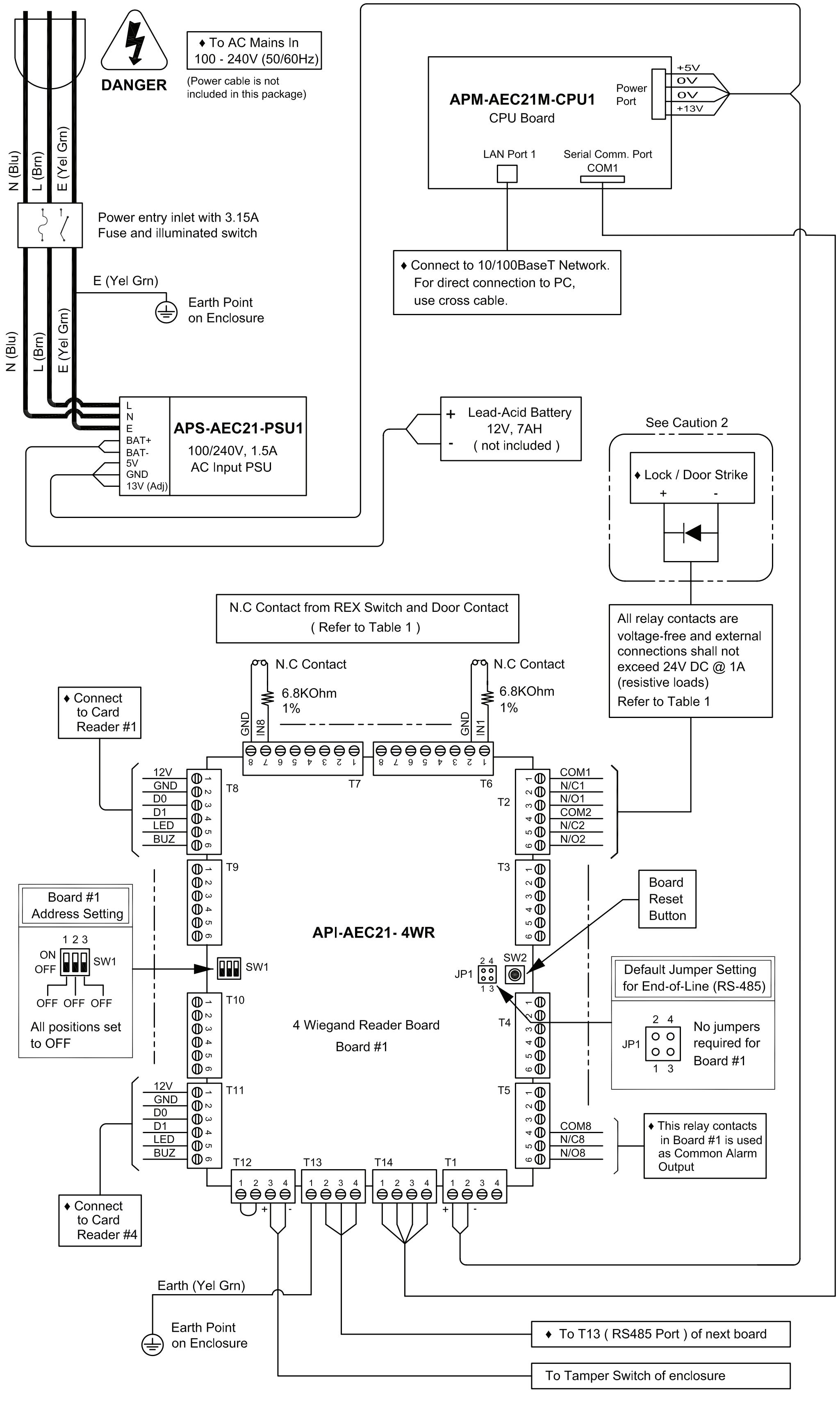
Figure 19.1 Inter-connection of the components within the main controller panel

Location	Cable Type
AC Input socket to PSU	0.75mm 2 x 3 (18 AWG) Core Insulated (Black) Power Cable, Length 220mm, PVC Insulated
RJ45 to CMC, directly or via hub	UTP Category 5 Cable
PSU output to CPU board	18 AWG, 4-conductors, unshielded
Back-up Battery	18 AWG, 2-conductors, unshielded
CPU to 4-Reader boards	24 AWG, 4-Conductors Data Cable, shielded
Interface boards to Interface boards	RS485- 24 AWG, Cat5e, 4-conductors, shielded
Tamper Switch	24 AWG Twisted Cable Pair (2x White), unshielded
Card Readers to interface board (4-Reader board)	22 AWG, 6-conductors, unshielded
Input devices to input terminals of interface boards (4-Reader and 8-IO boards)	22 AWG, 2-conductors, unshielded
Output devises to output terminals of interface boards (4-Reader and 8-IO boards)	18 AWG, 2-conductors, unshielded

Note: The specification above is based on recommended minimum requirements. Shielded cables are recommended for outdoor and/or noisy environments.

UL listed and/or recognized wire must be used for cabling and wire suitable for the application.

The wiring diagram below shows the power limited and non-power limited circuits. There should be a minimum 0.25 inch separation between power limited and non-power limited circuits.


DANGER
♦ To AC Mains In
100 - 240V (50/60Hz)
(Power cable is not included in this package)
N (Blu)
L (Brn)
E (Yel Grn)
Power entry inlet with 3.15A Fuse and illuminated switch
E (Yel Grn)
Earth Point on Enclosure
L
N
E
BAT+
BAT-
5V
GND
13V (Adj)
APS-AEC21-PSU1
100/240V, 1.5A AC Input PSU
APM-AEC21M-CPU1
CPU Board
Power Port
+5V
0V
0V
+13V
LAN Port 1
Serial Comm. Port COM1
♦ Connect to 10/100BaseT Network. For direct connection to PC, use cross cable.
+ Lead-Acid Battery 12V, 7AH
- (not included)
See Caution 2
♦ Lock / Door Strike
+ -
All relay contacts are voltage-free and external connections shall not exceed 24V DC @ 1A (resistive loads)
Refer to Table 1
N.C Contact from REX Switch and Door Contact (Refer to Table 1)
N.C Contact
6.8KOhm 1%
GND
IN8
IN1
T7
T6
♦ Connect to Card Reader #1
12V
GND
D0
D1
LED
BUZ
T8
T9
T10
T11
T2
T3
T4
T5
COM1
N/C1
N/O1
COM2
N/C2
N/O2
Board Reset Button
Board #1 Address Setting
1 2 3
ON
OFF
SW1
OFF OFF OFF
All positions set to OFF
API-AEC21- 4WR
4 Wiegand Reader Board
Board #1
JP1
SW2
2 4
1 3
Default Jumper Setting for End-of-Line (RS-485)
No jumpers required for Board #1
COM8
N/C8
N/O8
♦ This relay contacts in Board #1 is used as Common Alarm Output
T12
T13
T14
T1
1 2 3 4
+
-
♦ Connect to Card Reader #4
Earth (Yel Grn)
Earth Point on Enclosure
♦ To T13 (RS485 Port) of next board
To Tamper Switch of enclosure

20 Appendix D Selecting A Correct Battery Size

This section provides information on choosing the correct battery for the AEC2.1 system.

20.1 Battery Specification for Access Easy Controller 2.1

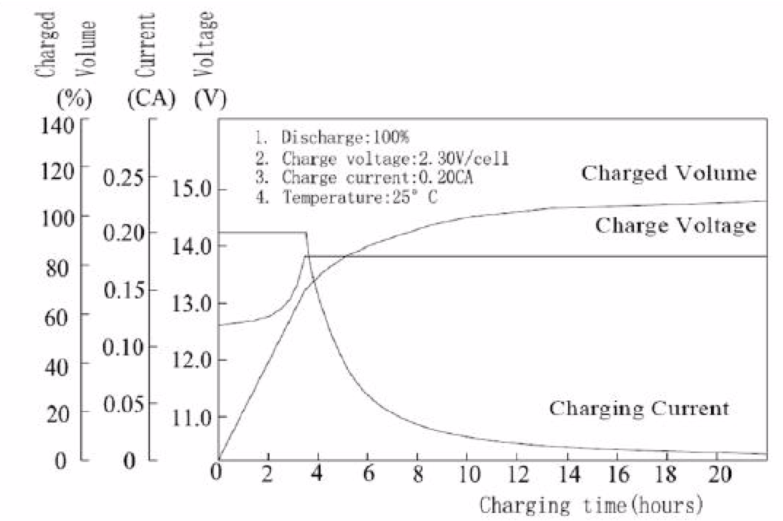
The following battery specifications are recommended for the use of AEC.

Specifications

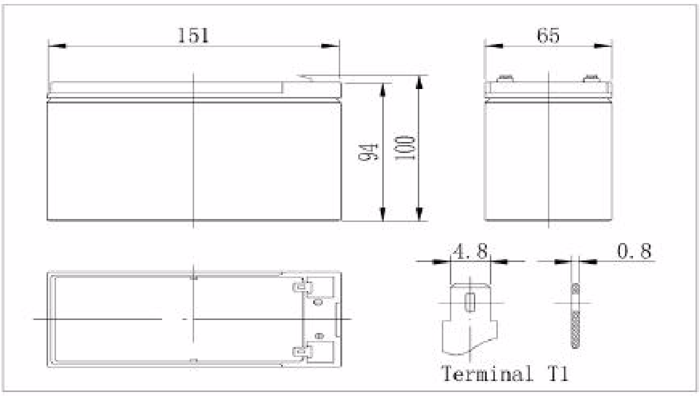
Nominal Voltage		12V
Capacity (20HR, 25°C)		7 Ah
Dimension	Length	151mm (5.94 inch)
	Width	65mm (2.56 inch)
	Height	94mm (3.70 inch)
	Total Height	100mm (3.94 inch)
Approx. Weight		2.35Kg (5.18 lbs)
Internal Resistance (Fully Charged, 25°C)		Approx. 25mΩ
Capacity affected by temperature (20HR)	40°C	102%
	25°C	100%
	0°C	85%
	-15°C	65%
Self-discharge (25°C)	3 month	Remaining capacity: 91%
	6 month	Remaining capacity: 82%
	12 month	Remaining capacity: 65%
Nominal Operating Temperature		25°C ± 3°C (77oF ± 5oF)
Operating Temperature range		-15°C ~ 50°C (5oF ~ 122oF)
Float Charging Voltage (25°C)		13.60 to 13.80 V
Cyclic Charging Voltage (25°C)		14.50 to 14.90 V
Maximum Charging Current		2.1 A
Terminal Material		Copper
Maximum Discharge Current		105 A (5sec)

WARNING!
There is a danger of explosion if the battery is incorrectly placed. Replace only with the same type of battery recommended.

Charging Characteristics (25°C)



Dimensions



Constant Current Discharge Characteristics (A, 25°C)

F.V/TIME	5min	10min	15min	30min	60min	3h	5h	10h	20h
9.60V	27.4	18.0	14.0	8.20	4.70	1.83	1.24	0.71	0.37
10.2V	26.0	17.1	13.4	7.86	4.55	1.80	1.22	0.70	0.36
10.8V	24.4	16.1	12.7	7.46	4.35	1.76	1.20	0.68	0.36

Constant Power Discharge Characteristics (Watt, 25°C)

F.V/TIME	5min	10min	15min	30min	60min	3h	5h	10h	20h
9.60V	305	203	160	92.0	54.4	21.7	14.8	8.52	4.43
10.2V	290	191	153	88.2	52.7	21.4	14.6	8.40	4.37
10.8V	273	180	145	83.8	50.4	21.0	14.3	8.17	4.32

21 Appendix E Troubleshooting

21.1 Login Problems

This section offers troubleshooting guidance for situations when you can successfully connect to the AEC2.1, but the login process fails.

The following list summarizes the warning and error messages that could be displayed while attempting to log in to the AEC2.1. For each message, refer to the indicated paragraph of this section for information concerning cause and remedial action.

MESSAGE	**REFER**
Login failed	*Section PROBLEM 1: Login Failed., page 102*
No such user name	*Section PROBLEM 2: No such user name., page 102*
Incorrect password	*Section PROBLEM 3: Incorrect password., page 102*

PROBLEM 1: Login Failed.

Symptom: When attempting to login to the controller for the first time, the message “**Login Failed**” is displayed.

Possible causes:

1. Wrong user name or password entered. The default user id is **user1** and password is **8088**.

2. The browser's security setting is set too high. AEC2.1 runs a Java script that encrypts and protects user ids and passwords when they are passed over the network. Verify that the Java feature is enabled in the browser.
   - With Internet Explorer, click **Tools** > **Internet Options**; then select the **Security** tab. In the **Internet Zone** section, the security level is probably set to High. Change the security level to Medium, then click the **Apply** button to activate the change. Now, close and reopen Internet Explorer to establish a new connection to the AEC2.1.

PROBLEM 2: No such user name.

Symptom: From the AEC2.1 Login screen, the message “**No such user name**” is displayed when you click the Login box after entering the user id and password.

Possible cause:

The user id that you are attempting to login with is not in the controller's database.

If this is a new user id, then probably the database was not backed up to flash memory after the user account was created.

Try logging in using the master user id and password. Assuming these have not been changed from the default values, the default master user id is **user1** and the password is **8088**.

PROBLEM 3: Incorrect password.

Symptom: From the AEC2.1 Login screen, the message “**Incorrect password**” is displayed when you click the Login box after entering the user id and password.

Possible cause:

You are entering the wrong password for the user id.

- Passwords are case sensitive. Be sure you are typing upper and lower case characters correctly.
- If the password for the user id was recently changed, perhaps the database change was not saved. Try the old password.
- Perhaps the user forgot the password. Log in using any other user id that has database administrative privileges. Then change the password for the user in question. Save the database after making the change.

21.2 Network Connectivity Problems

This section offers troubleshooting guidance for situations when you are unable to communicate with the AEC2.1 over the customer's network.

Be sure to follow the steps below in order when diagnosing the cause of the connectivity problem. Do not skip any steps.

Step 1 - Confirm the controller's compatibility with the customer's network

Procedure:

Review the AEC2.1 application checklist to confirm the controller's compatibility with the customer's network. The application checklist can be found in *Section 23 Appendix G Blank Configuration Form, page 116* of this manual.

Decision:

Can a “**Yes**” answer be confirmed for all questions in the application checklist?
Yes - Proceed to step 2.
No - AEC2.1 will not work in your application. Have the customer make corrections as suggested in the application checklist, then re-start this procedure. If the customer cannot make the suggested corrections, then an alternative access control solution should be suggested.

Step 2 - Confirm that the basic AEC2.1 is operating correctly

Procedure:

1. Observe that LED 9 on the interface board is blinking. This shows that the processor on the interface board is operating.

2. Observe LED 10 and LED 11 located on the interface board. These LEDs should be blinking. This shows that the CPU is interacting with the interface boards.

3. Observe the Green LED on the RJ45 jack on the CPU board. It should be lit steady.

4. Observe the Amber LED on the RJ45 jack on the CPU board. It should be flickering momentarily.

Decision:

Did all indicators perform as described in this step?

Yes - Proceed to step 3
No - There is a basic problem with the controller. Replace the interface board

Step 3 - Verify that the AEC2.1 can connect directly to the technician's computer

Procedure:

1. Disconnect the controller from the customer's network.

2. Connect the AEC2.1 directly to the technician's computer using the crossover CAT5 cable.

3. Confirm that the technician's computer is configured for IP address similar to the AEC2.1 e.g. if the AEC2.1 has an IP address of 192.3.0.66 and Subnet Mask of 255.255.0.0, then the technician's computer has to have an IP address of 192.3.0.X (For example 192.3.0.67) and Subnet Mask of 255.255.0.0. The Gateway address field should be blank.

4. Connect to the AEC2.1 using the Web browser on the technician's computer. The Login screen should be displayed.

Decision:

Can a connection be made to the controller?

Yes - Proceed to step 4
No - Verify the configuration of the technician's computer. Also, check the cable between the AEC2.1 and the technician's computer.

Do not proceed further in this test procedure until you are able to establish connectivity between the controller and the technician's computer.

Step 4 - Verify that the AEC2.1's network settings are configured correctly for the customer's network

Procedure:

1. Connect to the AEC2.1 using the technician's computer and login using the master id and password (user id: **user1** and password: **8088**).

2. Go to the controller **System** > **Network Setting** page and review the Controller's IP address, Subnet Mask and Gateway.

Decision:

Are the network settings correct for the customer's network?

Yes - Proceed to step 5.
No - Set the controller address by performing the following steps in the order described.

1. Go to **System** > **Network Setting**s and enter the correct network settings, and click the **Save** button to save the settings.

2. Reboot the controller.

3. After the power up sequence has been completed, reconnect the controller to the customer's network using the straight-through CAT5 cable and test connectivity from the customer's computer. If the controller still cannot be reached, repeat this test procedure beginning with step 3.

Step 5 - Verify that the wall jack or hub into which the AEC2.1 is connected properly.

Procedure:

1. Configure the technician's computer that was used in the previous step to the exact same network settings as the AEC2.1. Be sure to reboot the computer after making the TCP/IP configuration changes.

2. Disconnect the AEC2.1 from the customer's network and connect the technician's computer in its place. Be sure to use the same wall jack (or hub port) as used by the controller. Also, use the same category-5 cable, used to connect the controller to the hub. Be sure to use a straight-through cable, not the crossover cable that was used in the previous steps of this procedure.

3. Check the indicator LED on the customer's hub for the port to which the technician's computer is connected.

Decision:

Is the green LED lit for the hub port to which the technician's computer is connected?

Yes - The wiring between the computer and the customer's hub is correct. Continue with step 6.
No - On most hub, a yellow or red LED usually indicates cabling problem between the computer and the hub. A non-lit LED usually indicates an open circuit between the computer and the hub. You may want to try a different cable, or a different hub port. Also, be certain the computer is not connected to an Upstream port on the hub.

Some hubs may have indicators different from those described in the preceding paragraph. Refer to the hub's documentation for additional details.

Do not proceed further in this test procedure until this step can be passed.

Step 6 - Validate network configuration using the “ping” command

Procedure:

With the technician's computer still connected to the customer's network, and the hub port indicating a “green” condition, have the customer use one of the network connected computer's to send a “ping” command to the address of the technician's computer. The “ping” command should be performed from a computer on the same local sub-net as the technician's computer.

Decision:

Did the customer receive a response to the “ping” command?

Yes - Proceed to step 7.
No - There is a network configuration problem.

If the “ping” command returned the message “Request timed out,” then there is a basic network configuration error, possibly the setting of the IP address or subnet mask assigned for the AEC2.1. Or the customer's router may not be configured properly. Review these items with the customer.

If the “ping” command returned the message “Network unreachable”, then the customer's router or proxy server may be configured incorrectly, or the IP address, netmask, or gateway provided for the AEC2.1 are incorrect.

In either case, do not proceed further in this test procedure until this step is successfully passed.

Step 7 - Confirm that the technician's computer can “ping” the customer's computer and/or gateway on the same local sub-network.

Procedure:

From the technician's computer, open a DOS window and send a “ping” command to a customer computer on the same local subnet. Ideally, you should “ping” the computer that was used in the previous steps.

Question:

Was a response received to the “ping” command?
Yes - Proceed to step 8.
No - There is a network configuration error.

If the “ping” command returned the message “**Request timed out**”, then there is a basic network configuration error. Probably sub-net mask or gateway assigned for the AEC2.1 is incorrect. Or the customer's gateway or router may not be configured properly.

If the “ping” command returned the message “**Network unreachable**”, then the IP address or netmask of the controller may be wrong.

If the computer uses a gateway, try to “ping” the gateway from the technician's computer.

If a response is received, then the customer's gateway or router may have a configuration problem.

If no response is received, then the gateway address provided by the customer is incorrect, or the gateway is not operating correctly.

Step 8 - Reconnect the AEC2.1 to the customer's network and test it by using the “ping” command from the customer's computer.

Procedure:

1. Disconnect the technician's computer from the network and reconnect the AEC2.1. Be sure to use the same wall jack or hub port, and the same cable as used with the computer.

2. Have the customer use one of his network connected computer's to send a “ping” command to the address of the AEC2.1. The “ping” command should be performed from a computer on the same local subnet as AEC2.1. Ideally, it should be the same computer used in the previous two steps.

Decision:

Did the customer receive a response to the “ping” command?

Yes - Proceed to step 9
No - One or more basic problems still exit. Repeat this procedure beginning with step 2.

Step 9 - Confirm that the AEC2.1 can be reached using a Web browser

Procedure:

1. From the same customer computer used in the previous step, have the customer use the Web browser to connect to the AEC2.1. The AEC2.1 Login screen should be displayed.

Decision:

Yes - Proceed to step 10.
No - One ore more settings are incorrect in the Web browser.

Check the general connection setup, and proxy settings.

Also, set the browser's security setting to medium. If set on high, connection may be prevented under certain circumstances.

Be certain the browser is attempting to connect over a LAN. Often, the browser may be defaulted to attempt connection over a dial-in network.

If still unable to connect, try another computer.

Step 10 - Log on to the AEC2.1

Procedure:

1. Enter the super user user id **user1** and password **8088** to log on to the AEC2.1. Upon successful login, the controller's home page should be displayed.

Decision:

Was the login successful?

Yes - Problem solved.
No - The controller is working properly. However, one or more settings are incorrect in the Web browser. Continue with the next Chapter, Troubleshooting Login Problems, for guidance in resolving browser settings.

22 Appendix F Frequently Asked Questions

The AEC2.1 is targeted for small to mid-sized users who, because of the expense traditionally associated with access control solutions, have not been able to justify such systems in their security plans. While AEC2.1 performs all the traditional access control functions, it also introduces some new concepts never before seen in an access control product.

The controller is unique in a number of ways. First, it interfaces to a host computer using the customer's network. Second, a standard Web browser, such as Microsoft Internet Explorer, provides the user interface to the controller. No special application software is needed. Third by using only industry standard HTML pages, database management tasks are the easiest of any access control controller on the marketplace today. Fourth is the video verification option that allows you to view Live or Playback videos. And fifth, AEC2.1 offers a low-cost solution that will fit the budget of most small businesses.

In order to help you understanding the AEC2.1 product, we have compiled a list of most frequently asked question concerning the installation, operation and capabilities of the AEC2.1.

22.1 General Questions

Question - My old access control system requires a user to be logged on and monitor the system at all times. Does a computer always need to be connected to the AEC2.1?

Answer - No. The only time a computer needs to be connected to the AEC2.1 is when it is necessary to make database changes or review transaction history or when the user wants to monitor the controller activity. Other than these, it is not necessary to be logged into, or connected to, the AEC2.1.

Once database has been set up, the AEC2.1 will function indefinitely without user attention. Unlike some access control systems, there are no buffers that will fill up and overflow if the controller is not tended to at periodic intervals.

Question - I would like my receptionist to monitor the AEC2.1 during business hours, but she has other applications that need to be running on her computer. Can the AEC2.1 be monitored in the background without affecting the receptionist's ability to run other programs, such as MS Word and Excel?

Answer - Definitely. The receptionist can login to the AEC2.1, open the Transactions screen, and select the desired setting (Alarm, Valid, Restore or All). Then minimize the Transactions window.

Now the receptionist can open and run other applications, such as MS Word or Excel.

When AEC2.1 detects an alarm condition, the audible chime will sound to alert the receptionist to the alarm. The receptionist can then restore the Transactions screen and handle the alarm without disturbing any of the other work. When finished with the alarm, the receptionist needs to minimize the Transactions and be ready to continue working with the other application.

Question - I noticed that some of the AEC2.1 graphic and text presentation are slightly different when displayed on my associate's computer when compared on my computer. Is this normal?

Answer - This is normal. Screen displays will vary slightly depending on which browser program you run. Different browser display certain HTML code differently from one another.

Also, within browsers, there are some slight differences from one revision of the browser to the next. It is recommended to use Microsoft Internet Explorer, version 7.0 and above with AEC2.1.

If you are using an older version of the browser, then we recommend that you upgrade to a more current version.

Another item that can cause noticeable differences from one computer to the next is the screen resolution setting. The AEC2.1 pages have been designed to work best with a screen resolution of 1024x768.

Question - Can the AEC2.1's database be backed up off the controller, perhaps to a diskette, in case the controller should suffer a massive failure of any type? I would hate to have to manually re-enter the entire card database for our 500 employees. Also, if I can back up the controller's database to a diskette, is there a way to restore the database back into the controller?

Answer - Yes to both questions. The AEC2.1's database can easily be saved to a computer, either on the hard disk or a diskette. To perform a database backup to a computer, simply follow the instructions on the Database Backup section of the software manual.

Question - When I am monitoring the AEC2.1, I notice that the Transactions screen only displays the ten most recent records. Is there any way to increase the number of records displayed at one time on the Transactions screen?

Answer - Yes. The number of records to be displayed on the Transactions screen can be increased by increments of 10 up to a maximum of 70.

Changing the value is easy. A person with administrative privileges will need to go to the controller **Activity** > **Default Settings** page. Select the number of transactions from the **Number of Transactions to View** dropdown menu. After selecting the desired value, click the “save” button to store the change.

The change will be effective immediately. If anyone is running the Transactions screen at the time the setting change is made, that person will need to exit the Transactions screen and re-enter it to take advantage of the change.

Question - My old access system uses HID proximity readers and cards. Can AEC2.1 replace my old access system without changing the HID proximity reader and cards?

Answer - Yes, as long as the HID proximity readers provides wiegand output and you know the card format of the cards, you can replace your old access system with AEC2.1 without changing the readers and the card. Refer to the AEC2.1 Software User Manual for details in configuration card formats.

Note: 26 bit card formats are evaluated by UL.

22.2 Controller Questions

Question - For how long will a fully charged battery maintain AEC2.1 operation during a power failure?

Answer - Assuming that the standard 12 Volt, 7.0 Amp hour supplied with the controller is fully charged, it will typically provide four hours of operation during a power outage. This estimate is based on a controller configured with two 4-Reader boards, each with four readers connected to it, for a total controller configuration of eight readers. The estimate also assumes that the readers are HID ProxPro, MiniProx or ProxPoint models.

A controller configured with other than the HID model readers listed above will typically experience less operational time to standby batteries. Likewise, a controller configured with less than eight readers can be expected to operate for a slightly longer time on standby power.

Question - I would like to install an expansion chassis at the other end of the building from where the controller is located. This will make for shorter cable runs from the expansion controller to the readers at the end of the building. What is the maximum between the expansion chassis from the main chassis?

Answer - As the expansion chassis can be connected in the RS485 loop, you could locate it to a maximum of 1Km away from the main chassis.

Question - Can I get separate controller Tamper alarms for the main AEC2.1 and the expansion controllers?

Answer - Yes, each controller Tamper can be terminated to the Tamper alarm input of the interface boards in the Controller. This way you will have individual Controller's tamper monitored separately, however, whenever there is an activation from either one of the tamper, the AEC2.1 will announce as controller tampered.

Question - Can the AEC2.1 work with normally closed alarm devices? I already have normally closed door contacts in place that I would like to monitor with the AEC2.1.

Answer - Yes. Normally closed devices will work with AEC2.1. AEC2.1 can monitor both normally open and normally closed devices. The controller database is defaulted to expect normally open type devices; however, it is an easy task to change the setting of any input point to expect normally closed type operation.

Question - The CPU board was faulty and I did backup the latest soft copy of the database. Is there any other way I could recover my data?

Answer - Yes, if fault was not due to the compact flash memory card, we could just replace the AEC2.1 CPU and insert the previous compact flash memory card and the system will work as per previous configuration.

22.3 Reader and Door Questions

Question - What is the maximum cable length between the AEC2.1 and any card reader?

Answer - The maximum cable length between the controller and the reader is 150m when using the recommended Paige 6-conductor shielded cable. Maximum cable length will be less when using non-standard cable.

Question - Reader 1 through 4 were easy to install and make operational. However, I am having difficulty getting the readers above 4 to operate. What could be causing this?

Answer - This is probably a database issue because all AEC2.1 contain reader board 1, the database is defaulted with the first four readers enabled. When adding additional reader boards to the controller, you will need to activate the additional readers in the database before they will start working.

To do this, select **Configuration** > **Device** > **Door** from AEC2.1 menu. Then, from the reader list select the reader that you want to make operational. When this reader's detail screen is displayed, click the **Next** button to go to the second page of detail data.

If you look at the Scheduling Options section on this page, you will see that **Unlock Door** is selected. Deselect Unlock Door by choosing one of the other scheduling options; then click the Save button to save the modified record. The reader should now be operational.

Question - There is a beeper in HID MiniProx reader that sounds each time a card is presented to the reader. On interior doors this beeper is annoying. Can it be turned off?

Answer - No. The HID MiniProx reader offers no option to disable the beeper. The best solution in areas where the beeper is annoying is to install a ProxPro reader. The ProxPro reader has a setup switch that will disable the beeper.

Question - I can't get a green LED indication on a ProxPoint reader when access is granted as a result of a valid card read. Why is this?

Answer - Early production of the ProxPoint reader did not provide for control of the green LED. The solution is to either replace the ProxPoint reader with a later production model that includes green LED support, or replace the ProxPoint reader with a MiniProx reader.

Question - The motion detector that I am using as my request-to-exit sensor performs inconsistently. It will work the first time a person approaches the door to exit, but may not work at all when a second person approaches the door some 10 to 15 seconds later. What is wrong?

Answer - There is nothing seriously wrong. This is a common occurrence with certain models of motion detectors.

The reason is because some motion detector models take up to 30 seconds or longer to reset after detecting motion. This is done to minimize swinging alarm situations when the motion detector is connected to an intrusion alarm system. Until the motion detector resets after detecting the first motion, it will not detect any subsequent motion. We suspect this may be the reason the detector fails to react when a second person approaches the door closely behind the first person.

The solution is easy. Most motion detectors that exhibits this operational characteristic have a switch or jumper setting that you can change which will allow the detector to immediately reset after the motion, which activated the detector, has cleared. You will need to check the manufacturer's documentation for the motion detector model that you are using to make this jumper change.

Question - All my reader controlled doors are interior doors to offices and stockrooms. Will the AEC2.1 work correctly if door contacts are not installed on these doors?

Answer - The controller will work just fine. Door contacts, while usually installed, are optional with AEC2.1. Realize, however, that without installing contacts, the controller will be unable to detect and report Door Held Open and Door Forced Open conditions form these doors.

Question - What should be done if an employee has forgotten his/her PIN code?

Answer - The Administrator should login to AEC2.1, locate the employee's records, reassign a new PIN code and inform the employee. The employee can then change the new code at any Readers with keypad.

Question - What should be done if an employee report that he/she cannot access a door after presenting his/her card?

Answer - The Administrator can check the Transactions screen for the record and determine the cause of the denied access.

Example 1: Transaction shows “**Access Denied**”, this shows that the employee has no access rights to the door.

Example 2: Transaction shows “**Invalid Schedule**', this shows that the employee is not allowed to access this door during this time period.

Example 3: Transaction shows "**Access Denied - Passback**", this shows that the employee did not present the card to the exit reader when the employee exited from the door (the employee could have followed someone through the door).

22.4 Inputs and Outputs

Question - Can the controller also monitor doors that do not have readers connected to them, such as emergency exit doors?

Answer - Yes. We would install contacts on these doors and connect them to an 8-Input-Output board. The AEC2.1 can support up to four of these boards. Each board is capable of monitoring eight points of protection. Depending on specific controller configuration, an expansion chassis may be needed to house the 8-IO board(s).

Question - What is the maximum wire length between 8-IO board and an alarm sensor?

Answer - When using standard 22-gauge burglar alarm cable, the maximum cable length is 500m.

Question - Can glass break detectors be connected directly to an input on the 8-IO board?

Answer - No. In most instances, this will not work. The reason is because alarms from many glass break detectors are often of very short duration. The AEC2.1 circuitry must see the alarm condition exist for 500 ms before it will recognize and respond to the alarm.

Glass break sensors should be wired to a controller, and the controller should provide the connection to AEC2.1.

22.5 Network Question

Question - How many computers can be connected to the AEC2.1 at the same time?

Answer - Typically, only one computer is connected to the AEC2.1 at a time. However, the controller will continue to provide satisfactory performance with two concurrent user sessions running.

Bosch Security Systems recommends that concurrent controller logins be limited to two to provide rapid response to user requests for information. While the controller will handle more than two concurrent logins, the users may notice degradation in the speed with which screen pages are drawn when there are multiple simultaneous logins to the controller.

Question - What is the maximum cable length between the AEC2.1 and the network hub to which it is connected.

Answer - Since this cable is industry standard category-5 Ethernet cable, the length is limited to 100 metres. Bosch Security Systems recommends that you do not exceed this cable length. If a longer cable run is needed, then Ethernet extenders should be used to increase the distance.

For a UL compliant installation, the following installation guidelines must be followed.

The controller must be installed in the same room as the network jack or hub.

Note: UL listed and/or recognized wire must be used for cabling and wire suitable for the application.

23 Appendix G Blank Configuration Form

This chapter provides blank configuration form for 4-Reader boards or 8-IO boards. The System Installer could use them to plan the set up before commencing on the installation. This form will also help the Installer doing the AEC2.1 programming to assign the correct address to devices in the system.

AEC2.1 Boards Configuration Page ___ of ___

4-Reader Board

SW1 Address Settings:	
Reader Ports	Reader Number / Description (e.g. Reader #1 / Door 1)
T8-1 to T8-6	
T9-1 to T9-6	
T10-1 to T10-6	
T11-1 to T11-6	
Input Channels	Device Connected / Description (e.g. Exit Push Button for Door 1)
T6-1 and T6-2	
T6-3 and T6-4	
T6-5 and T6-6	
T6-7 and T6-8	
T7-1 and T7-2	
T7-3 and T7-4	
T7-5 and T7-6	
T7-7 and T7-8	
Output Channels	Device Connected / Description (e.g. Door Strike for Door 1)
T2-1 to T2-3	
T2-4 to T2-6	
T3-1 to T3-3	
T3-4 to T3-6	
T4-1 to T4-3	
T4-4 to T4-6	
T5-1 to T5-3	
T5-4 to T5-6	

Prepared By: ___________

Date: _______

AEC2.1 Boards Configuration Page ___ of ___

8-IO Board

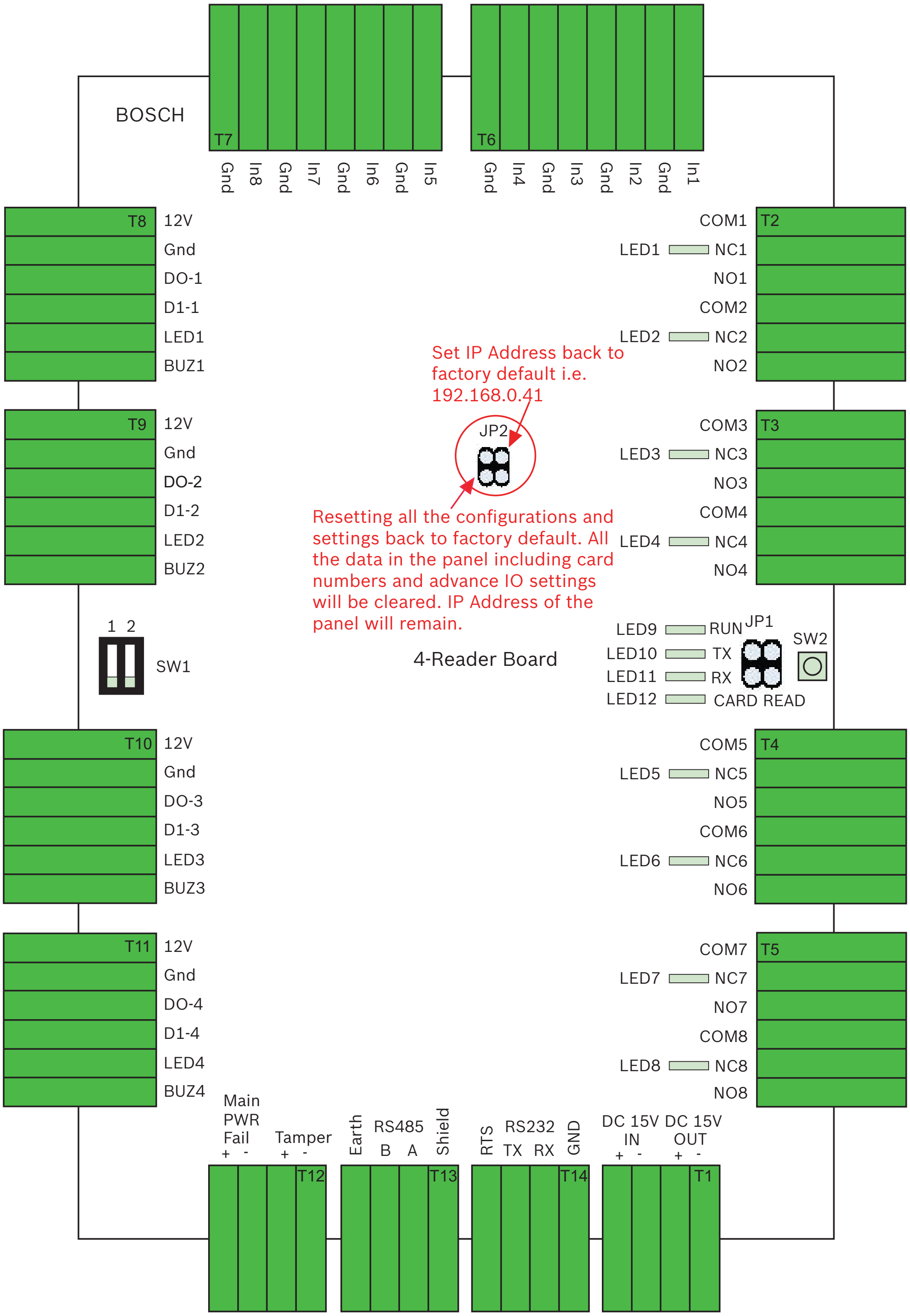
SW1 Address Settings:	
Input Channels	Device Connected / Description (e.g. PIR at Warehouse)
T6-1 and T6-2	
T6-3 and T6-4	
T6-5 and T6-6	
T6-7 and T6-8	
T7-1 and T7-2	
T7-3 and T7-4	
T7-5 and T7-6	
T7-7 and T7-8	
Output Channels	Device Connected / Description (e.g. Alarm Status for PIR)
T2-1 to T2-3	
T2-4 to T2-6	
T3-1 to T3-3	
T3-4 to T3-6	
T4-1 to T4-3	
T4-4 to T4-6	
T5-1 to T5-3	
T5-4 to T5-6	

Prepared By: ___________

Date: ___________

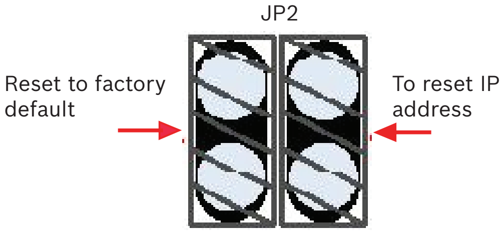
24 Appendix H Resetting to Factory Default

On the first 4-Reader board of AEC2.1 system, JP2 is used to reset the panel to factory default setting.



Set IP Address back to factory default i.e. 192.168.0.41

Resetting all the configurations and settings back to factory default. All the data in the panel including card numbers and advance IO settings will be cleared. IP Address of the panel will remain.



NOTICE!

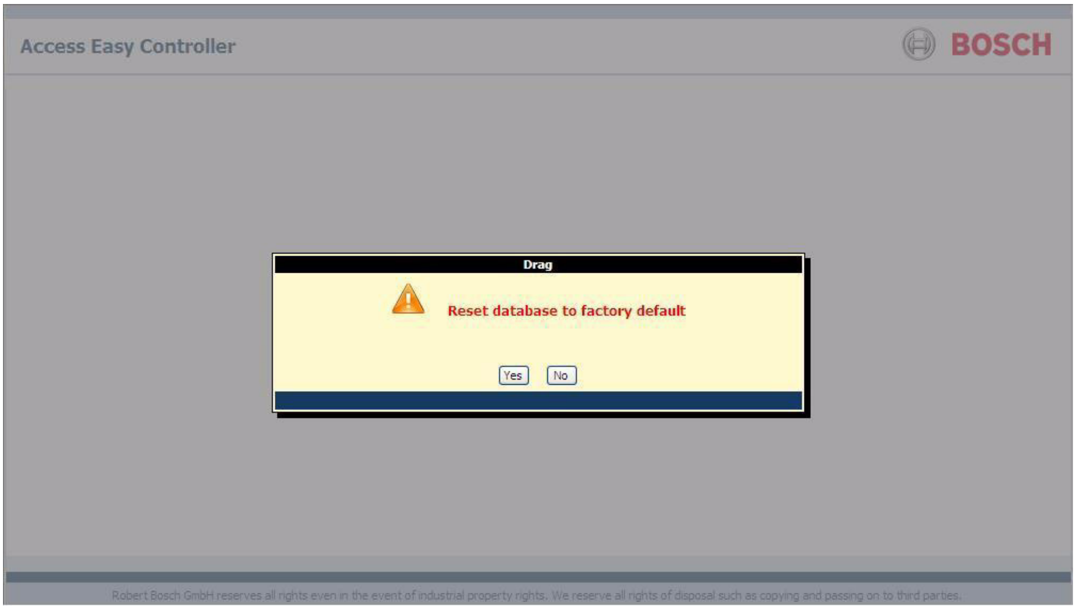
These two functions are independent of each other and can be carried out independently or simultaneously.

- Shorting the jumper on the left and rebooting the system will cause the panel to be reset to factory default settings, keeping the IP Address unchanged. Refer to *Section 24.1 Resetting to Factory Default, page 119* for more information.
- Shorting the jumper on the right and rebooting the system will cause the panel to reset ONLY the IP Address to default IP Address.
- Shorting both will reset both the, configurations and settings, and IP Address.

24.1 Resetting to Factory Default

When the jumpers on the left of JP2 (vertically), is shorted with a jumper link the system provides the option to retain the current settings and configuration or clear all the settings and configuration.

When the jumpers are shorted the screen below appears.


Access Easy Controller

BOSCH

Drag

Reset database to factory default

Robert Bosch GmbH reserves all rights even in the event of industrial property rights. We reserve all rights of disposal such as copying and passing on to third parties.

Click the **Yes** button to reset the AEC2.1 back to the factory default settings. This process will clear all the settings and configurations set, except for the IP address. Information like Card numbers and Advance IO settings will also be erased.

WARNING!

- All information, settings and configurations will be erased. Users are advised to do a system backup before proceeding. (IP Address will not be reset with this function)

Click the **No** button to reboot the panel without changing the settings and configurations.

After setting the jumper link the system will reboot. Upon system reboot, enter the AEC2.1 URL address in the address field of a web browser.

24.2 Resetting IP Address to Default IP Address

The jumpers on the right of JP2 (vertically), when shorted with a jumper link, will reset the panel’s IP address back to AEC2.1 default IP address (i.e 192.168.0.41). Note that this will only reset the IP Address back to default. No information, settings and configurations will be altered. A reboot will be required for changes to take effect. Upon completion of rebooting, you will be able to log onto the login screen with the default IP Address.

Robert Bosch (SEA) Pte Ltd
11 Bishan Street 21
573943 Singapore
Singapore
www.boschsecurity.com