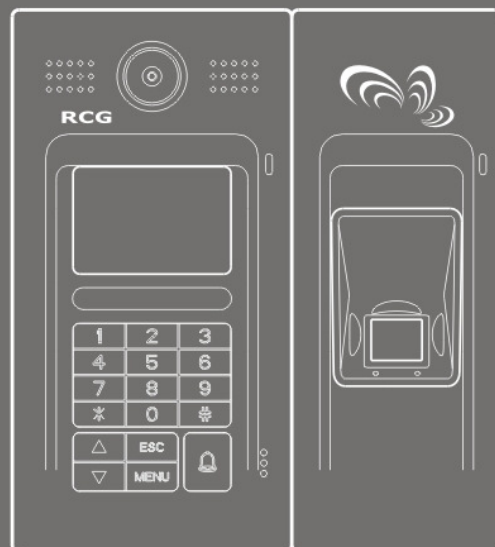


RCG
Biometrics • RFID • Security

i4 FLEXI

Multi-Functional Access Control System
Installation Guide



RCG i4 Flexi Installation Guide V2.1

This is an operating manual for i4 Flexi Access Control & Time Attendance Management System. Every attempt has been made to make it accurate as possible. However, product changes will occur from time to time and please refer to our web site for latest updates. While RCG has attempted to make this document as accurate as possible, we expressly disclaim any and all warranty of accuracy and completeness, and accept no liability for any loss or damage arising from any inaccuracies or omission.

Please send comments to [**support@rcg.tv**](mailto:support@rcg.tv)

Federal Communications Commission (FCC) Statement

This Equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Trade Name: i4 Flexi

Model No: PTN-100206-01-A



Conventions

This guide uses the following conventions:



This icon denotes particularly important information.



This icon denotes precautions to avoid injury, data loss, or a system crash.



This icon denotes precautions to avoid a burn hazard.



This icon denotes precautions to avoid being electrocuted.

bold Bold text denotes items that you must select or click on in the software, such as menu items and dialog box options. Bold text also denotes parameter names.

Italic Italic text denotes emphasis, a cross reference, or an introduction to a key concept. This font also denotes text that is a placeholder for a word or value that you must supply.

Table of Contents

1	About i4 Flexi.....	7
1.1	Key Components.....	8
1.2	Features	9
1.2.1	Characteristics	9
1.2.1.1	Enhanced Security.....	9
1.2.1.2	Reliable and stable algorithm.....	9
1.2.1.3	Entrance security	9
1.2.1.4	Function keys and log records	10
1.2.1.5	Low system maintenance cost.....	10
1.2.1.6	One system to control several terminals.....	10
1.3	Support functions.....	11
1.4	Definitions	12
1.5	Operating Sensor	14
1.6	System Specifications	15
2	Hardware (main board).....	17
2.1	Connector description	17
3	Safety Information	21
4	Installation	23
4.1	Physical Connection.....	23
4.2	Precautions	24
4.3	Installation - Preparations.....	24
4.4	Where to install	25
4.5	Power Requirements.....	25
4.6	Installing i4 Flexi.....	25
4.7	Wall Installation.....	26
4.8	Fastening.....	26
4.9	Cabling	27
5	Application example.....	28
5.1	Standalone.....	28
5.2	PC – RS 232	29
5.3	PC – TCP/IP.....	31
5.4	PC – RS 485	32
5.5	Wiegand.....	34
5.6	RF module connection.....	36
5.7	Alarm connection.....	37
6	Configuration.....	39
6.1	Basic Flow	39
6.2	How to enter the administration menu.....	41
6.3	Network	42
6.3.1	Terminal ID	43
6.3.2	Controller SN	44

6.3.3	Network Mode.....	45
6.3.3.1	TCP/IP.....	45
6.4	User Registration.....	46
6.4.1	How to register user	46
6.4.2	Fingerprint registration.....	47
6.4.3	Activate FP, Card, Password Access Mode.....	48
6.5	Use & Authentication method.....	49
6.6	System with Wiegand Connection	50
6.6.1	Wiegand Content.....	50
6.6.2	Wiegand Input	51
6.6.3	Wiegand Output.....	52
7	Tips and precautions.....	53
7.1	First setting in initial use	53
7.2	Difficult fingerprints	53
7.3	Reset i4 Flexi and return to setting status before last trial.....	53
7.4	Right fingerprint registration position.....	53
7.5	Cleaning the Sensor	54
7.6	Sensor Maintenance Warnings.....	54
8	Appendix 1 - i4Flexi Alarm Operation.....	55
9	Appendix 2 - Quick Start Procedure & Drawing	58
10	Glossary.....	61
11	Support Information.....	62

1 About i4 Flexi

i4 Flexi Access Control & Time Attendance Management System is a powerful tool for access control and time attendance management. i4 Flexi adopts with latest optical fingerprint sensor and high-precision fingerprint identification algorithm. With supports of RS485 (converter required) and TCP/IP protocols, it can be implemented as both standalone and networked.

i4 Flexi adopts separate controller and centralized connection board design to enhance security. Tamper alarm will go off if an intruder try to open the device and alarm relay output can be generated.

With its Wiegand Input and Output features, the system can be easily reinforced by just adding an external reader. (Optional Wiegand Input– 26 bit or 34 bit). The i4 Flexi device can also act as a reader to send out Wiegand signal to existing controller. (Optional Wiegand Output feature – 26 bit or 34 bit). This offers more choices to end users.

i4 Flexi boasts an attractive appearance with changeable casing design. It is easy to operate, ready to implement and embedded with various innovative features. By using high resolution and blue backlit LCD, clear and attractive image can be display. The keypad is made of durable material and so heavy-duty usage is not a problem. Its built-in voice system provides an interactive operation mode.

i4 Flexi can store up to 5,000 fingerprints and supports 1:1 & 1:N identification. Its offers seven verification modes, namely Fingerprint only, Password Only, Card only, fingerprint or password, Card and fingerprint, Card and password, Card and Fingerprint and Password.

1.1 Key Components

i4 Flexi Fingerprint Access Control System has two main components: A Main Unit and a door lock controller.

Main Unit: Manages registration and storage of user data, query and setting of system information, verification of fingerprint data, recording and storage of log information, and display of prompt information. It consists of fingerprint processor module, LCD, keypad, doorbell button, fingerprint sensor, reset button and casing. The interface of the fingerprint main unit (hereinafter referred to as the “equipment”) is shown in the diagram below.

- Product’s appearance description

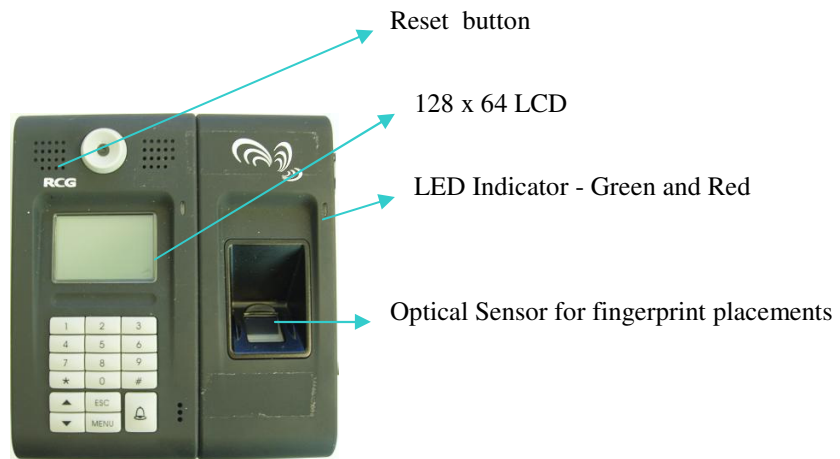



Fig. 1 Appearance of i4 Flexi

‘#’	Enter key: Confirm your present operation
MENU	Menu key: Press down the key for seconds to enter the management interface in the initial state
ESC	Cancel key: Cancel your present operation
OUT/▲	Scroll up key: Scroll up the menu & OUT: Check for off work
IN/▼	Scroll down key: Scroll down the menu & IN: Check for on work
‘*’	Clear key: Clear the input
	Door bell button (providing dry contact for external door bell)
0 – 9 :	Numerical key.

Lock control unit: The control centre of the lock controller. It is also the execution component of the i4 Flexi. It controls the locking and unlocking of the door lock based on the instructions of the fingerprint processor, monitors door lock state of the access control system, and triggers alarm signals in the event of security breaches.



Fig. 2 Lock Control Unit

1.2 Features

1.2.1 Characteristics

1.2.1.1 Enhanced Security

Traditional security systems such as smartcards and keypad locks are not always reliable, given the high incidences of loss and theft. With RCG's fingerprint recognition system, such problems can be easily eradicated. Because biometric technology is known to minimize crime and save time, i4 Flexi is a valuable tool to enhance security.

1.2.1.2 Reliable and stable algorithm

RCG created an unique, proprietary algorithms for i4 Flexi. The algorithms enable i4 Flexi to provide a high degree of fingerprint verification accuracy.

1.2.1.3 Entrance security

In addition to monitoring access control, i4 Flexi maintains a record of all visitors to an area and their time spent on premises. This system makes it possible for human resources and payroll departments to rely on accurate data to compute staff wages.

1.2.1.4 Function keys and log records

i4 Flexi has four programming keys to manage the time and attendance functions. With i4 Flexi, one single terminal can be assigned to manage access control and employees' time and attendance.

1.2.1.5 Low system maintenance cost

Traditional ID systems, such as the smartcard, can incur high long-term costs since replacements are necessary when staff or member cards go missing. i4 Flexi eliminates this long-term cost, given that it relies on employees' own biometry to identify them.

1.2.1.6 One system to control several terminals

One i4 Flexi module can function in standalone mode to monitor access control. i4 Flexi can also connect to other modules compatible with TCP/IP/RS232/RS485 modems to link to a central server. i4 Flexi is equipped with RTC technology, which allows it to log up to 10,000 records and manage access control without the use of an ACU adaptor.

1.3 Support functions

User management	<ul style="list-style-type: none"> ■ Register a user (RF, fingerprint, password) ■ Delete a user or all users ■ Query the number of registered users ■ Query the remaining capacity to register new users ■ Query ID allocation ■ Set a user's time zone ■ View registered ID list ■ Transmit user's data in software terminal
System management	<ul style="list-style-type: none"> ■ Configure and read terminal's time and date ■ Change and read security level ■ Change Terminal ID ■ Configure communication mode (TCP/IP, RS485) ■ Receive firmware version ■ Change lock operating time
Door mode	<ul style="list-style-type: none"> ■ Configure and read door mode (normal/ forced open/ forced close) and time
Log	<ul style="list-style-type: none"> ■ Log data contains the function key, entrance time and user ID ■ Query log count ■ Delete all logs
Authentication	<ul style="list-style-type: none"> ■ Terminal Authentication as 1 : 1, 1 : N and Grouping ■ Various authentication methods: RF, Password, Fingerprint, RF+FP, RF+PIN, FP+PIN and RF+FP+PIN
Auxiliary function	<ul style="list-style-type: none"> ■ Exit button ■ Relay in Lock driver ■ Transmit case status ■ Support voice message ■ Transmit door switch status
Alarm function	<ul style="list-style-type: none"> ■ Alarm Finger ■ Invalid Door Open Alarm ■ Tamper Alarm

Note:

1: 'Standalone' means that the management, registration and storage of user data, query and setting of system information, verification of fingerprint data, recording and storage of log information, and display of prompt information can be done once the fingerprint main unit is connected to a power source, and without the use of any networked PC.

1.4 Definitions

User: Users of i4 Flexi can be classified into two groups: User I and User II. User I refers to supervisors, managers, enrollers and normal users of i4 Flexi (hardware), and User II refers to PC software's (DAMS) users ("PC administrator") who can set and administer the data and parameters of i4 Flexi. The roles and responsibilities of the two groups of users are as follows:

1) User I: (User in i4 Flexi access control device)

"Supervisors", "managers", "enrollers" and "normal users" are end-users of i4 Flexi. These users are authorized to perform verification, enquiry and administration. "Normal users" have the authority to use the system only, whereas "supervisors", "managers" and "enrollers" have different levels of authority to administer the equipment.

User authority: The four user types of the equipment have different levels of authority, and are ranked as follows:

Supervisors > managers > enrollers > normal users

Normal users: Normal users do not have the authority to administer the equipment. They can only conduct operations such as access verification.

Enrollers: user who are entitled to enroll new users or delete an existing user in the system. They can't enter the "Menu->2.options" & "Menu->3.Network".

Managers: In addition to the operations that normal users can conduct, managers maintain some administrative authorities except those dedicated to "supervisors". Specifically, "managers" can add, delete, or modify the data of "managers" "enrollers" and "normal users" and they can check the verification logs of any user on the system. They can't enter the "Menu->2.options->1.system opt->5. adv. Opt" & "Menu-> 2. option -> 5. Auto Test" & "Menu -> 3.Network-> 3.com key".

Supervisors: Supervisors have the highest operating authority of the system. In addition to the operations that managers can conduct, supervisors can access the "system administration" of the system to set various setting parameters. Specifically, they can add, delete or modify the data of any user, or delete all the users so that the system reverts to its original empty state. **【Note: It is impossible to modify another supervisor】** .

2) User II : (User in DAMS software)

The PC administrator uses PC-based software tool to maintain the data of the access equipment, mainly the outputting and processing of access administration and the verification log, maintenance of access system parameters, and backup and restoring of user data,.

(Note: To access via the PC software, the equipment must be in the standby state to ensure successful connection.)

Empty state: The state in which i4 Flexi is void of any user; either no user data are stored in the main unit terminal (supervisor, administrator, enroller or normal user) or all user data have been deleted.

Standby state: i4 Flexi is idle or is not receiving any input signal from the processor, i.e., no button is pressed. On the LCD screen, only current date and time will be displayed.

Exit button: An optional feature of the i4 Flexi fingerprint access control system. It can be mounted inside a door, and a user can press on the button to unlock the door.

Offline use: With offline use, the fingerprint processor connected to the power supply can perform functions such as registration and storage of user data, query and setting of system information, verification of fingerprint data, recording and storage of log information and display of prompting information. These jobs can be done without the use of a PC.

Wiegand Output: Wiegand signals plus Wiegand controller may also control the door lock.

Online assistant administration: i4 Flexi provides connection to PC through RS485/TCP, so that customers can administer the access control system, set the various parameters, and backup and restore the user data at the PC. This enables a customer to easily administer multiple access systems.

To successfully achieve communication between the equipment and PC, some parameters of the fingerprint processor have to be set according to the descriptions about “communication” in the following text.

Local alarm: The buzzer inside the fingerprint unit sends out alert sounds alarm.

Remote alarm: i4 Flexi is connected to an alarm in a remote location (such as a security guard office). The alarm goes off in the event of security breaches. People nearby the access system cannot hear the alarm sound.

Alarm finger: When enrolling fingerprints, a user may specify a finger as the alarm finger (fingers not specified as alarm fingers are considered “normal fingers”). When the user applies this finger to conduct “verification for door opening” or “menu logging” operations, the system will produce remote alarm signals. Alarm finger is usually used in duress situations.

Normal door opening: User uses an authorized finger (normal finger or alarm finger) to conduct “verification for door opening” through the access control system, or opens the door via the “exit button”. This is called normal door opening.

Invalid door opening: Any door opening action other than normal door opening is called invalid door opening. For instance, someone opens the door using invalid methods such as prying open the door using a crowbar, or unlocks the door with a key (without fingerprint verification or pressing the door release button).

Card, Fingerprint and password verification: i4 Flexi supports verification of card, fingerprint and password separately as well as combined verification of card, fingerprint and password. Separate card/password verification is useful for situations when a user’s fingerprint is difficult to register or validate due to its poor quality. The combination of card, fingerprint and password verification can improve the security of the whole system.

Finger relevancy: To enhance the user’s level of security, he/she may enroll two normal fingers and a set of two finger relevancies (both enrolled fingers must be used for verification), or register three normal fingers and choose to set two or three finger relevancies (two or three enrolled fingers must be used for verification). Once finger relevancies are set, the user must pass the verification for all finger relevancies to open the door when conducting fingerprint verification.

FRR: “False Rejection Rate” or FRR is measure of the probability the access system will wrongly reject an access attempt; the system will refuse the access attempt from an authorized user. A smaller percentage value reflects a better system.

FAR: “False Acceptance Rate” or FAR is a measure of the probability the access system will wrongly accept an access attempt; the system will accept the access attempt from an unauthorized user. A smaller percentage value reflects a better system.

1.5 Operating Sensor

When using the fingerprint sensor avoid touching the sensor surface with any sharp or hard object (be careful when installing the device). Always keep the surface clean. For cleaning, dip clean absorbent cotton in water and apply laterally to the stain.

Position of finger placement

To get a clear fingerprint image, place finger closely on sensor in the correct position as shown in the first two diagrams from the left in Fig. 3:

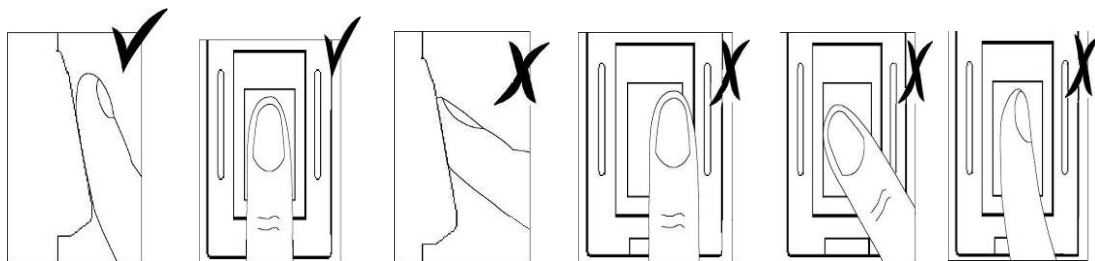


Fig. 3

The first two diagrams show correct finger placement. The other diagrams illustrate incorrect finger placements.

1.6 System Specifications

◆ Technical specifications

Item	Technical parameter
Type of sensor	Optical sensor
Resolution of sensor	500dpi
Effective area of sensor	18mm×16mm
Dimension of fingerprint processor	156 m (H) X 160 mm (W) X 38 mm (D)
FRR	$\leq 1\%$
FAR	$\leq 0.0001\%$
Finger matching time (1:1 matching)	$\leq 0.5S$
Verification mode	Fingerprint only, Password Only, Card only, fingerprint or password, Card and fingerprint, Card and password, Card and Fingerprint and Password
Verification mode	1:1, 1:N
Working mode	Standalone or Network
Output	1 x Relay output, 1 x Alarm Relay output
Max user capacity	5000 users (if 1 fingerprints per user)
Max fingerprint capacity	5000 fingerprints (10 fingerprints per user at most)
Max log capacity	50000 logs
Communication Protocol	TCP/IP, RS232, RS485, Wiegand (Input or Output)
Working temperature	0°C ~ 45°C
Working humidity	RH 20% ~ 80%
Working Voltage	DC 12V

Working Current	400mA
Relay Output (Lock, Alarm)	NC/NO connection, 3A/12Vdc or 120VAC
Time Zone	50
Group	50
Holiday Table	50
User / Group Association	Support
Forced Door Open/Close Schedule	Support
Alarm Type	Tamper Alarm, Alarm on threat (alarm finger), Invalid door open alarm
Wiegand	Support Wiegand input / Wiegand output (26 bit or 34 bit)
Other Features (Optional)	RFID Module
Language	English / Simplified Chinese / Traditional Chinese

© RCG Holdings Limited 2007 All rights reserved. Any reproduction, copying of the contents or any part of this Manual for any purpose without the prior written consent of RCG is strictly prohibited. While every care has been taken in preparing the contents, the Company expressly disclaims any warranty of accuracy and completeness Any change to the content may not be informed in advance.

2 Hardware (main board)

2.1 Connector description



Fig. 4 Main board

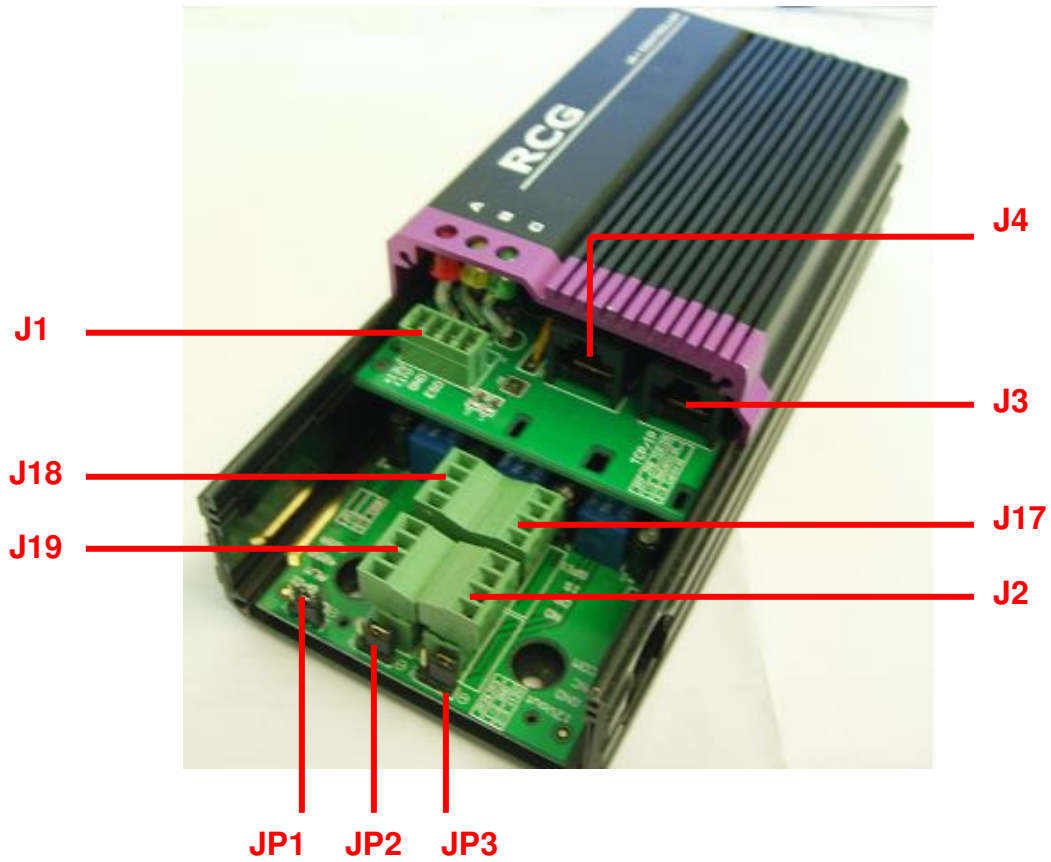


Fig. 5 Details on controller connectors

J1: Connect Power Supply

1	DC12V (Input)
2	GND
3	ESD

J3: Ethernet socket

RJ45

1	TX+
2	TX-
3	RX+
4	
5	
6	RX-
7	
8	

J4: Main unit socket

RJ45

1	TX+
2	TX-
3	RX+
4	GND
5	RXD
6	RX-
7	TXD
8	DC12V

J2: IO socket

1	DC12V: power (Output)
2	GND
3	NC: door lock Normal Close
4	COM: door lock COM

J17: IO socket

1	NO: door lock normal open
2	DS: door status input
3	IS; open button input
4	GPI1: General purpose input

J18: IO socket

1	WID0: Wiegand input D0
2	WID1: Wiegand input D1
3	WOD0: Wiegand output D0
4	WOD1: Wiegand output D1

J19: IO socket

12	RS485 A-
13	RS485 B+
14	ALARM: Alarm output
15	GPO1: General purpose output

JP1 : RS485 Termination resistor 120Ω – enable or disable

1-2 short : disable

2-3 short : enable

JP2 : General Output Port (GPO1), choose for GND or +12V connection

1-2 short : connect GND

2-3 short : connect +12V

JP3 : Alarm Output, select GND or +12V connection
 1-2 short: Connect GND
 2-3 short : Connect +12V

Indication Light

	Red Light	Yellow Light	Green Light
Lock Control Unit	Power Connected	Light blinking while traffic with processor	Door open

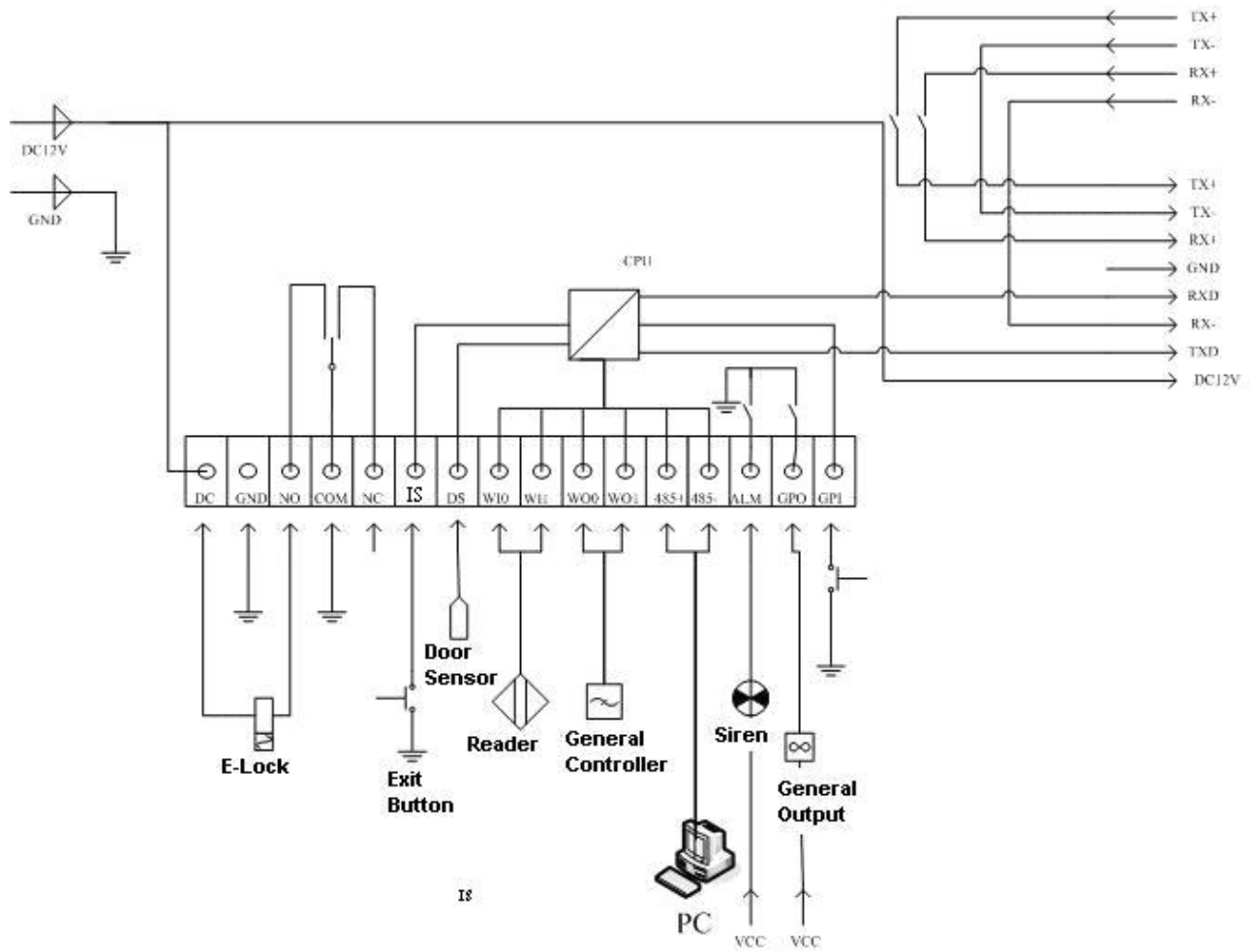


Fig. 6 Typical Connection with i4 Flexi controller

3 Safety Information



Caution The following section contain important safety information you *must* follow when installing and operating the device.

Do *not* operate the device in a manner not specified in the documentation. Misuse of the device may result in a hazard and may compromise the safety protection built into the device. If the device is damaged, turn it off and do *not* use it until service-trained personnel can check its safety. If necessary, return the device to RCG for repair.

Keep away from live circuits. Do not remove equipment covers or shields unless you are trained to do so. If signal wires are connected to the device, hazardous voltages can exist even when the equipment is turned off. To avoid a shock hazard, do not perform procedures involving cover or shield removal unless you are qualified to do so. Disconnect all field power prior to removing covers or shields.

If the device is rated for use with hazardous voltages, it may require a safety earth-ground connection wire. See the device specifications for maximum voltage ratings.

Because of the danger of introducing additional hazards, do not install unauthorized parts or modify the device. Use the device only with the chassis, modules, accessories, and cables specified in the installation instructions. All covers and panels must be installed while operating the device.

Do not operate the device in an explosive atmosphere or where flammable gases or fumes may be present. Operate the device only at or below the pollution degree. Pollution consists of any foreign matter—solid, liquid, or gas—that may reduce dielectric strength or surface resistivity. Pollution degrees are listed below.

- Pollution Degree 1—No pollution or only dry, nonconductive pollution occurs. The pollution has no effect.
- Pollution Degree 2—Normally only nonconductive pollution occurs. Occasionally, nonconductive pollution becomes conductive because of condensation.
- Pollution Degree 3—Conductive pollution or dry, nonconductive pollution occurs. Nonconductive pollution becomes conductive because of condensation.

Clean the device and accessories by brushing off light dust with a soft, nonmetallic brush. Remove other contaminants with a stiff, nonmetallic brush. The unit must be completely dry and free from contaminants before returning it to service.

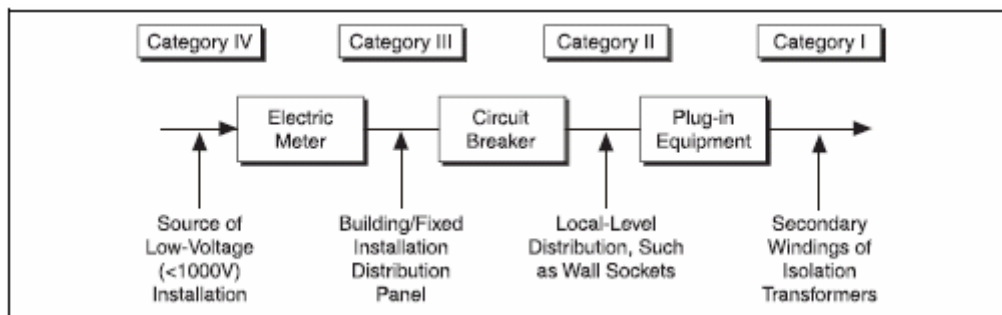
You must insulate signal connections for the maximum voltage for which the device is rated. Do not exceed the maximum ratings for the device. Remove power from signal lines before connection to or disconnection from the device.



You must operate the device **only below the installation category III**. The best practice is the main line having backup system. Installation categories are listed below.

- Installation Category IV—for measurements performed at the source of the low-voltage (<1000 V) installation. Examples include electricity meters, measurements on primary overcurrent protection devices, and ripple-control units.
- Installation Category III—for measurements performed in the building installation. Examples include measurements on distribution boards, circuit-breakers, wiring (including cables), bus bars, junction boxes, switches, socket outlets in the fixed installation, equipment for industrial use, and some other types of equipment, such as stationary motors permanently connected to the fixed installation.
- Installation Category II—for measurements performed on circuits directly connected to the low-voltage installation. Examples include measurements on household appliances, portable tools, and other similar equipment.
- Installation Category I—for measurements performed on circuits not directly connected to mains. Examples include measurements on circuits not derived from mains, and specially-protected (internal) mains-derived circuits.

The following is a diagram of a sample installation.



Caution A fire safety hazard exists when the total power dissipated by the power supply exceeds 36 W continuous for a sustained period of time.

4 Installation

4.1 Physical Connection

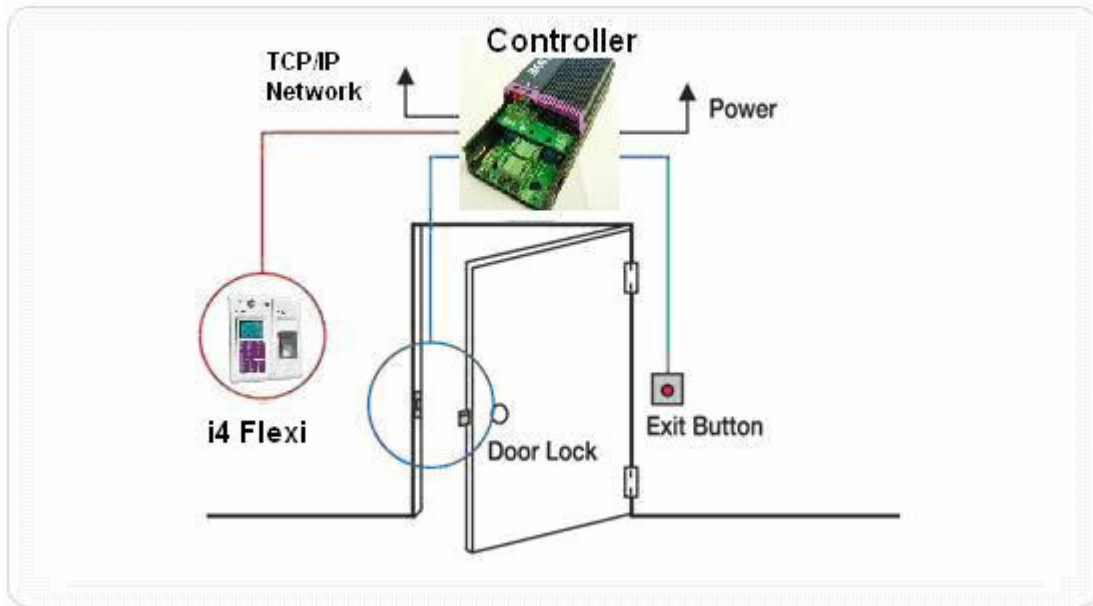


Fig. 7 i4 Flexi showing its main unit and controller

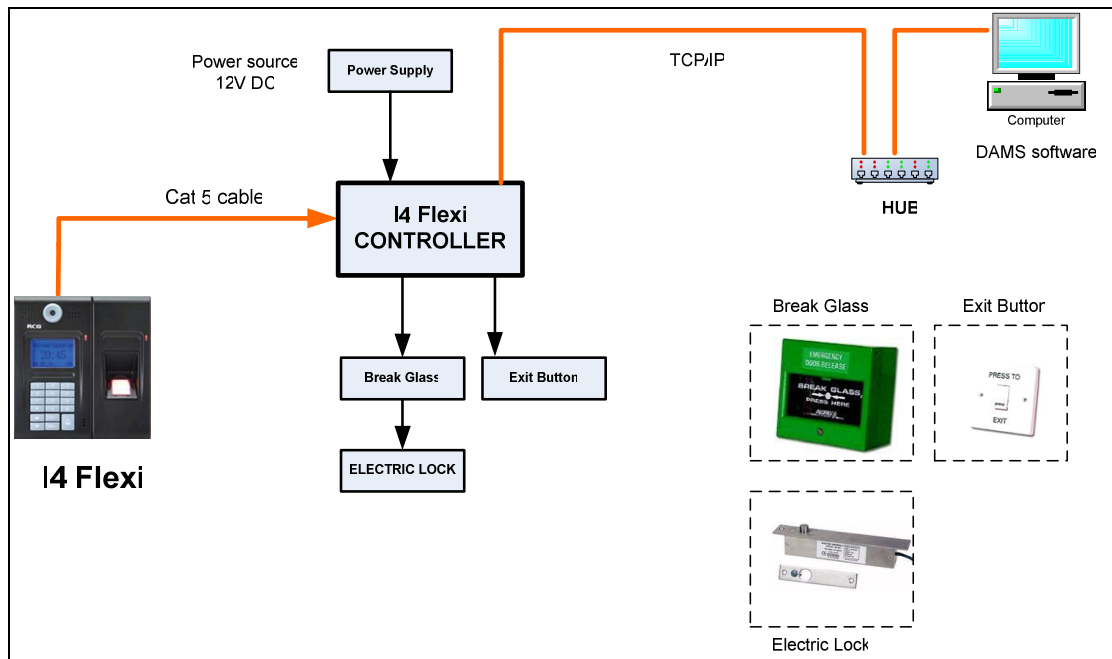


Fig 8 i4 Flexi System Diagram

The diagram shown above is typical TCP/IP connection of system, for another connection mode, please refers to section 5 “application example” for detail.

4.2 Precautions



Caution The following section contain important caution information you *must* follow when installing and operating the device.

Before installing i4 Flexi, users should read the following instructions.

Precaution Notes

- i4 Flexi is designed for indoor installation. When installed outdoors, i4 Flexi must be sheltered from water and concentrated humidity. i4 Flexi operates optimally at a temperature range of 0°C - 45°C
- i4 Flexi should be connected to a single power source to prevent short circuits or electrical shortages
- To increase security level, users should install the door controller at the door’s inner side
- The terminal should not be exposed to excessive heat and it should not be installed in dusty areas or those under direct sunlight.
- Do not place the controller under a water pipe or the Cooling Air Trucking system, as water leakage will harm the controller and potentially trigger a short circuit.
- Install i4 Flexi in such a way that the system has enough air circulation to prevent generated heat from accumulating inside the device.



Warning The Controller Relay Output rating is Max. 3A Capacity, users should take care the number of electric lock to be connected. Otherwise, the potential hazards of device burning or explosion will be much increased.

Warning The Power Supply Unit (PSU) consumption rating is depending of system consumption & PSU output capacity. Users should take care of PSU output capacity which is more than enough to provide the power to whole system. Otherwise, the potential hazards of device burning or explosion will be much increased.

4.3 Installation - Preparations

Choose the location where you plan to install the terminal, power controller, administrator computer, door lock, door button and power line. Inspect the following parts to ensure all system components are present and functional:

Items	Package List
1	Fingerprint Machine x 1
2	Controller x 1
3	i4 Flexi Installation Disk CD (DAMS) x 1 pcs
4	Installation Manual x 1 copy
5	Warranty Card
6	Door Bell Button Cable for external door button connection x 1 pcs

4.4 Where to install

i4 Flexi is a wall-mounting device. It is recommended that the device is placed as close as possible to the door to allow users to open it within the timeout period, which is set at default of five seconds.



Warning You have the option to install the device on a table. When installing, choose a sturdy, level surface in a ventilated area that is dust free and away from heat vents, warm air exhaust from other devices and direct sunlight. Avoid proximity to large electric motors or other electromagnetic equipment.

Observe the following guidelines when choosing a good location for the device:

- ✕ The surface must support at least 2kg.
- ✕ Temperature ranges from 32 to 113 degrees F (0 to 45 degrees C).
- ✕ Humidity should be less than 80%, non-condensing.
- ✕ Ventilation space should be 2 inches above and on each side, and 5 inches at the rear.
- ✕ Site should not exceed the electromagnetic field (RFC) standards for IEC 801-3, Level 2 (3V/M) field strength.
- ✕ 100 to 240 VAC, 50/60Hz power outlet should be within 6 feet of the controller.

4.5 Power Requirements

i4 Flexi is delivered without a power supply. Upon receipt, users must connect the controller to a DC 12V 3A Power Supply Unit. Communications and DC power are then transmitted via a Cat. 5 cable to the i4 Flexi terminal. Lock power comes from the power supply unit.



Warning: Do NOT use a separate power supply! Doing so will cause system failure or hinder operations.

4.6 Installing i4 Flexi

Avoid damage to the surface of i4 Flexi when using a screwdriver to open the cover.



Caution:

Star Key Wrench T10 is required to open the cover. 

Notice:

Cable distance for Ethernet Switching

The cable distance between device and hub/PC should not exceed 100 meter.

Cable distance for Device

The cable distance between device and controller should not exceed 50 meter. Using a high grade cable (individually shield low capacitance pairs), you can increase that distance to as much as possible with a good grade of cable.

Make sure the wiring is correct It can be used Category 3/4/5 cable in 10 Mbps operation. To reliably operate your network at 100Mbps, you must use an Unshielded Twisted-Pair (UTP) Category 5 cable, or better Data Grade cabling. While a Category 3 or 4 cables may initially seem to work, it will soon cause data loss. All kinds of hub/PC can connect to i4Flexi by using straight-through wires.

4.7 Wall Installation

Before installing i4 Flexi, ensure that the wall surface is clean and smooth [see Diagram 1]. Drill fixing and cable holes (for cable that will connect i4 flexi with the PC controller) at a height of 1.3 to 1.5 meters. *Please refer to appendix 2 for detail.*

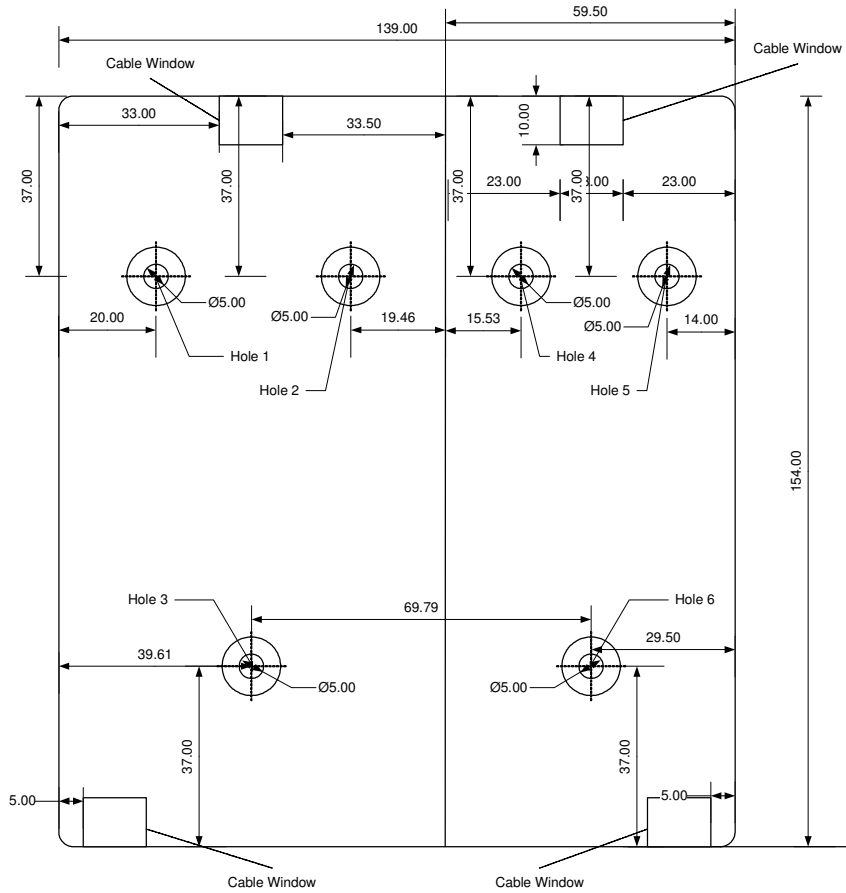


Fig. 9

Note: Place tapping screws ST3.5×25 in holes 1 to 6 to mount pad on the wall.

4.8 Fastening

Fastening 1, 2, 3, 4, 5, and 6 are fixing holes.

4.9 Cabling

Run a **Straight through Cat. 5 cable** to connect i4 Flexi to the controller. The cable is concealed inside a conduit; connect the cable directly to the RJ45 port inside the connection board.

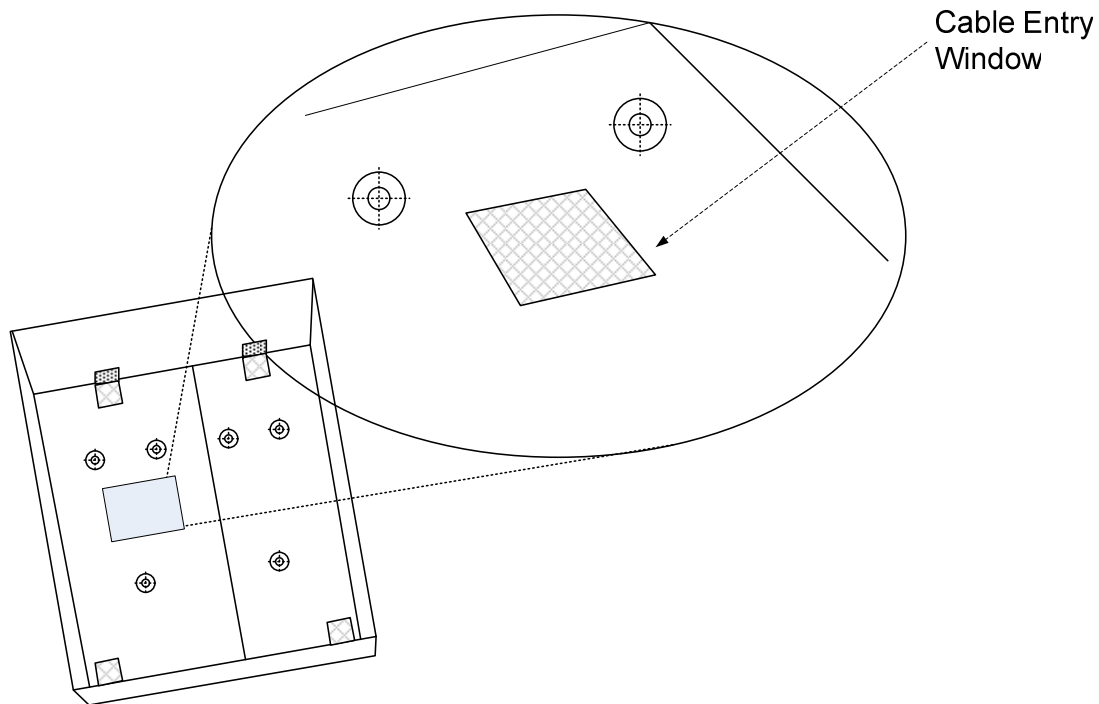


Fig. 10



Caution Be sure to turn off the power supply and the main AC power to your i4 Flexi and host computer *before* connecting the accessory to your controller.

Warning The i4 Flexi are energized when the power supply unit is powered on. Disconnect the i4 Flexi unit from the power outlet before connecting wires to or disconnecting wires from the controller connector. Strip back the insulation of the wires to the controller connectors no more than 7 mm. **Failure to do so could result in electric shock leading to serious bodily injury or death.**

Caution You must change the main input fuse on the front panel if you install the power cord into the back panel AC connector and plug it in to a correctly rated power source.

5 Application example

- Instruction for power line installation is not included
- Dead bolt, Striker, EM Lock and finishing will be shown here

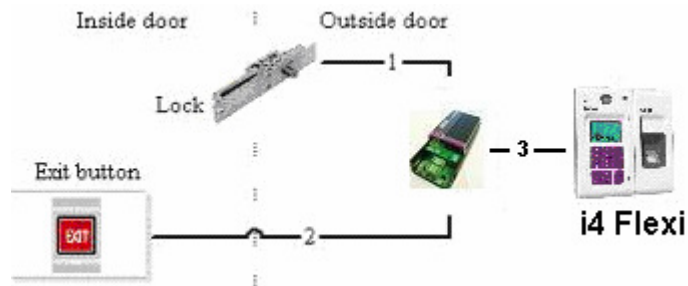
5.1 Standalone

- Install one unit only for access control without PC connection

Usage: Access control

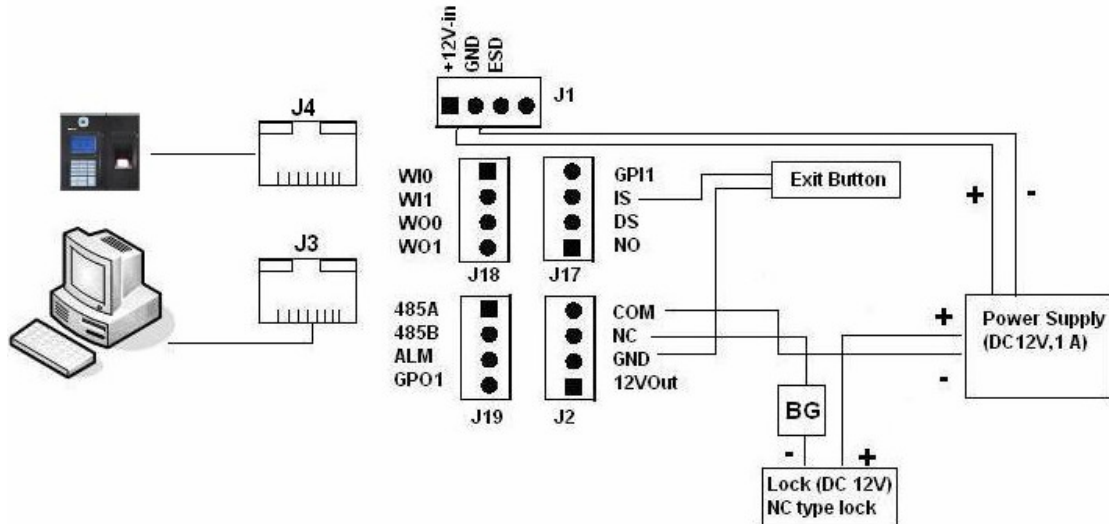
Configuration: i4 Flexi, Lock, inner exit button, S.M.P.S adapter (DC 12V 2A)

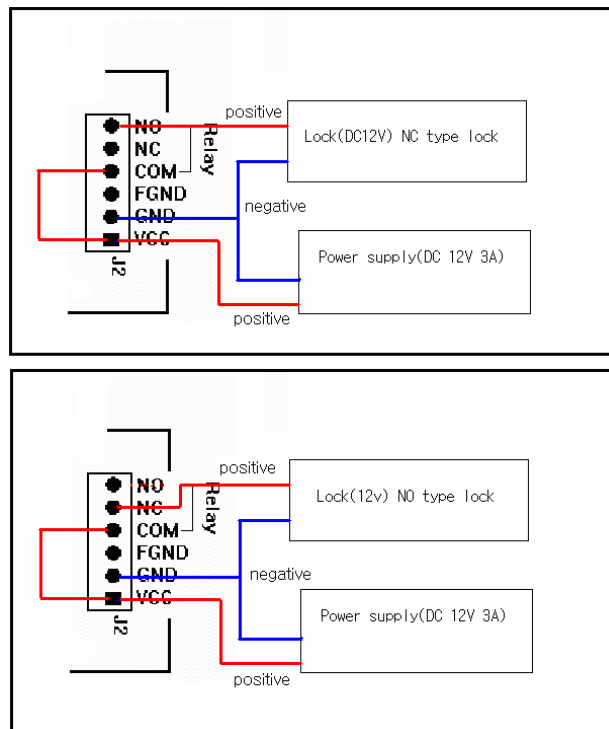
Block diagram



The number in the connection line means counting number of lines

Connection example of i4 Flexi connector





Connection example of NC/NO Lock

- Initial setting

Registration must be done at the i4 Flexi terminal, as instructed in section 5.1 of this manual.

5.2 PC – RS 232

Serial network application: When more than one i4 Flexi systems connect to a PC server via the RS-232 port. It enables access control and Time & Attendance management functions by software

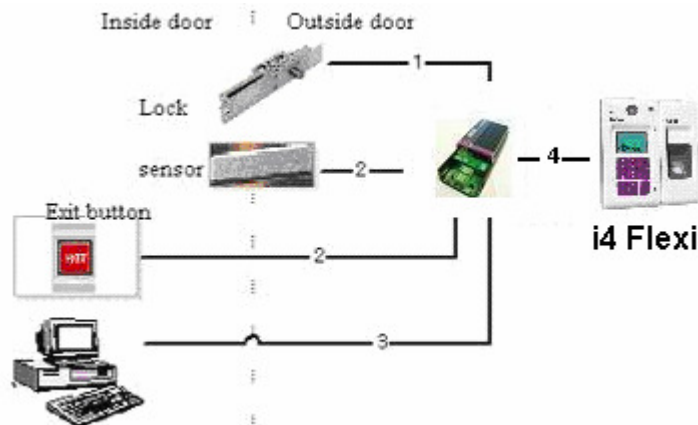
Configuration

Access control: i4 Flexi DAMS (terminal control & log management), Lock, inner exit button, S.M.P.S adapter (DC12V 2A), PC Server and door sensor.

Time & Attendance: i4 Flexi, DAMS (terminal control & log management), S.M.P.S. adapter (DC 12V, 2A) and PC Server.

Door sensor: Keeps track of when door is open or closed.

Block diagram

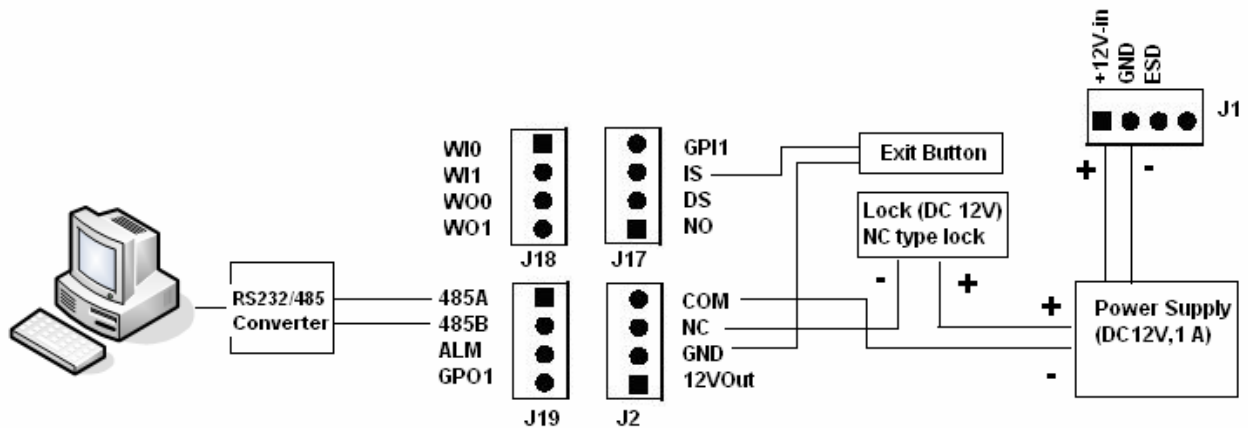




Cable distance for RS232

By using Cat.5 cable, the cable distance between device and controller should not exceed 50 meter. Using a high grade cable (individually shield low capacitance pairs), you can increase that distance to as much as possible with a good grade of cable.

Example of connection between i4Flexi and connector #2



Initial setting

- All settings are available on the PC and i4 Flexi, but for convenience, we recommend PC processing.

Registration

- Enroll users' fingerprints in i4 Flexi and downloads converted data to the PC server via D AMS.

Time & Attendance

- Users' event records are kept in i4 Flexi and transmitted to the PC server.
- In the PC, the DAMS program handles records according to clients' guidelines.

Door control

- Independent of terminal authentication, the door can be controlled in the compulsory mode of DAMS (open, closed, open/close timeframe).

Restriction of user admission

- All users' timeframe for admission can be set in DAMS. If users try to gain door access outside a set timeframe, the LCD window will show "It is not time to use" and shutdown all door functions.
- There are no time restrictions for users, unless a timeframe is manually inputted.

For more information on DAMS, please refer to the DAMS manual.

5.3 PC – TCP/IP

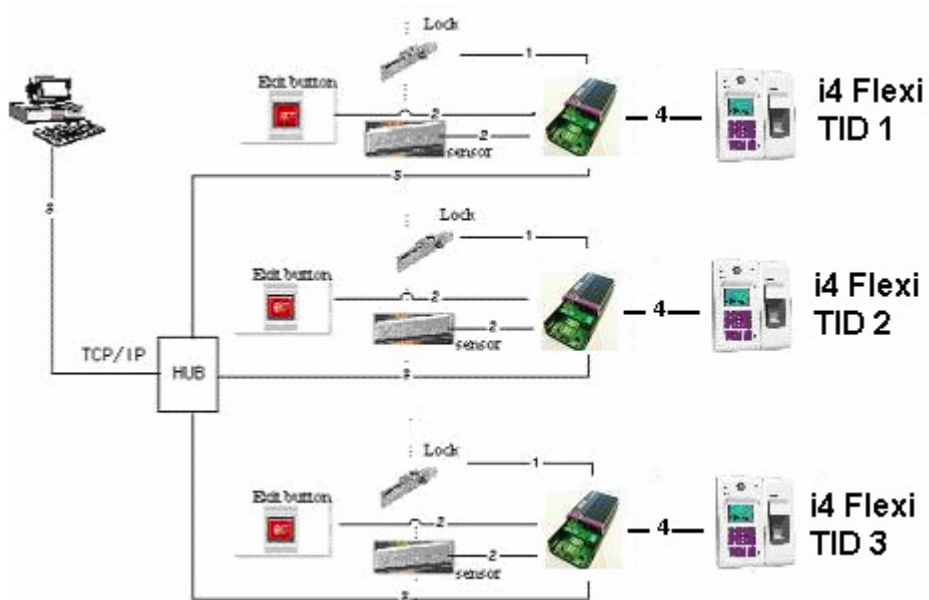
- i4 Flexi has a TCP/IP port that allows users to connect several terminals to a PC server network via HUB.
- In network mode, i4 Flexi should be linked to the TID (Terminal ID): 1 to 999. For more information on TID, please refer to section 11.1.1 of this manual.
- A straight thru cable is required to connect with PC & controller.

Configuration

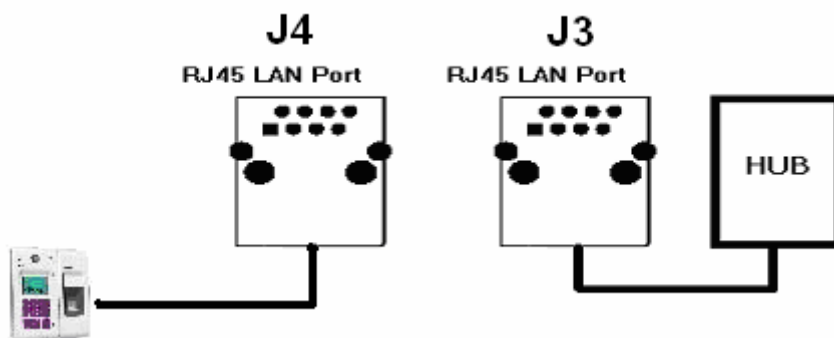
Access control: i4 Flexi, DAMS, Lock, inner exit button, S.M.P.S. adapter (DC 12V 2A), Server PC and door sensor

Time & Attendance: i4 Flexi, DAMS, S.M.P.S adapter (DC12V 2A) and PC Server

Block diagram



Example of i4 Flexi connecting systems



5.4 PC – RS 485

You can connect more than one i4 Flexi system with a PC via the RS485 port, but you need to use a converter to connect the RS232 and RS485 ports. To install more than one i4 Flexi, you must assign different TID numbers to each i4 Flexi unit. TID numbers range from 1 to 999. To change TID methods, follow the instructions in section 15 of this manual.

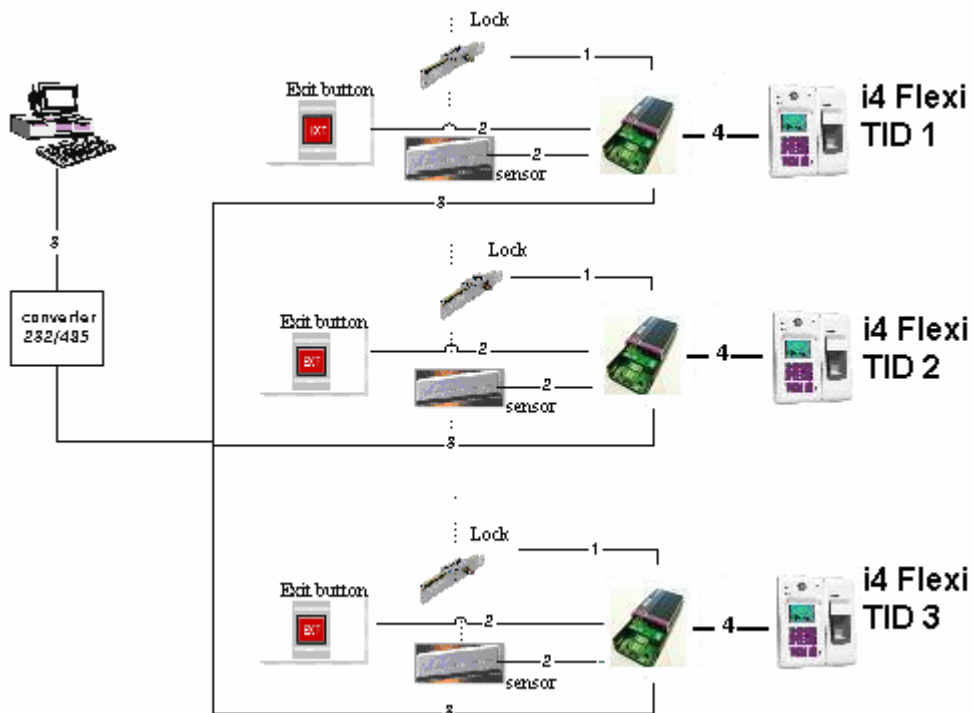
Configuration

Access control: i4 Flexi, RS232 to RS485 converter, DAMS (terminal control & log management), Lock, inner exit button, S.M.P.S. adaptor (DC 12V, 2A), PC Server PC and door sensor

Time and attendance: i4 Flexi, RS232 to RS485 converter, DAMS (terminal control & log management), S.M.P.S adaptor (DC 12V, 2A) and PC Server.

Door sensor: Keeps track of door status (open/closed).

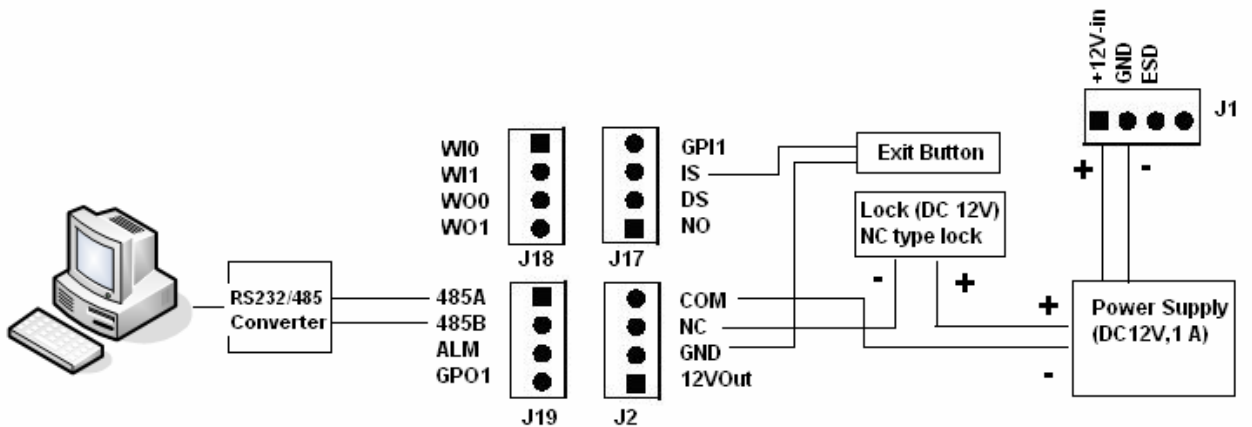
Block diagram



Cable distance for RS485

By using Cat.5 cable, the cable distance between device and controller should not exceed 1000 meter. Using a high grade cable (individually shield low capacitance pairs), you can increase that distance to as much as possible with a good grade of cable.

Illustration of i4 Flexi connecting systems



Connection example

i4 Flexi, converter connection specifications

i4 Flexi	232 to 485 converter
485 B+ (connector #1,4)	485+ (DSUB 25, 4)
485 A- (connector #1,3)	485- (DSUB 25, 6)
GND (connector #1, 5)	GND (DSUB 25, 2)

5.5 Wiegand

I4Flexi supports 2 kind of wiegand connection mode:

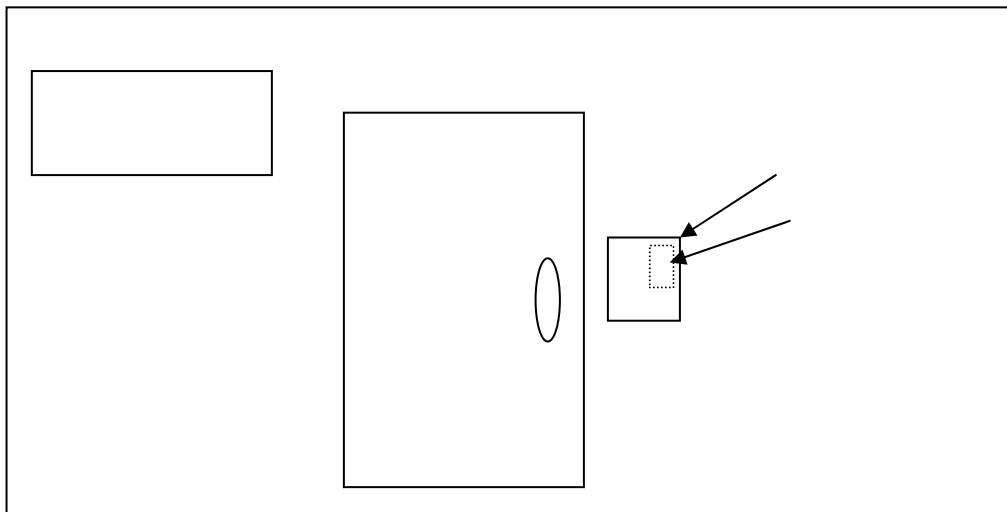
The **Wiegand input** is a function to build an application with external reader to form a professional access control. For example, some end user would like to change the front end input to be more accuracy data & enhance security. We may plug the i4 flexi with Access method RF+FP as entrance, while plug a RF reader as exit. (Example 1 -3)

The **Wiegand output** is a function to export transaction in real time to other access controller following the Wiegand standard 26 bit or 34 bit. When this is enabled, there should be another access controller connected with i4 Flexi's controller via Wiegand connection. It is the easier way to replace the existing card system but remains the aged controller as reporter and compatible aged HR software.

Example 1

(Built-in module, without external Wiegand reader)

Built-in RF Module Access Module: Follow the User Access Method (FP only, RF only, RF + FP, RF + FP + PIN etc.)

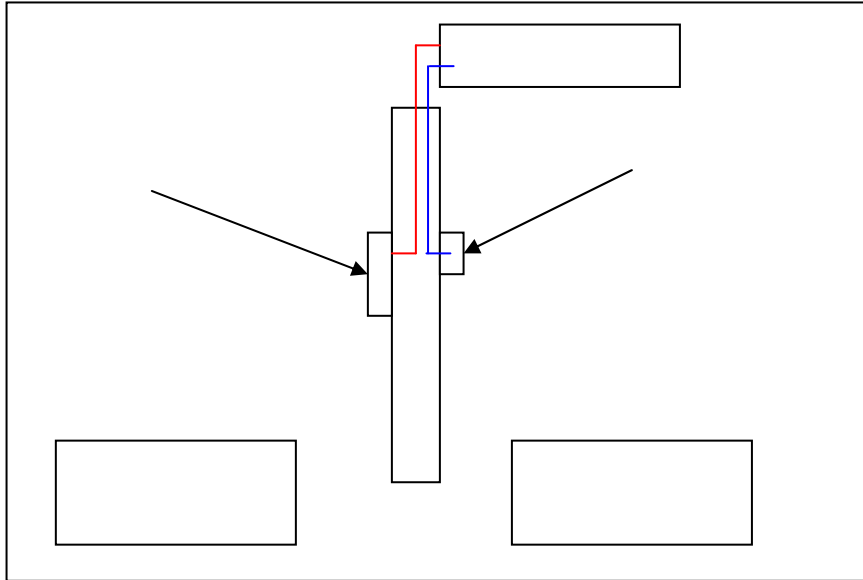


Example 2

(Built-in module + External Wiegand reader) <- *set the Wiegand Input as “In Door Read Card” mode*

Built-in RF Module Access Module: Follow the User Access Method (FP only, RF only, RF + FP, RF + FP + PIN etc.)

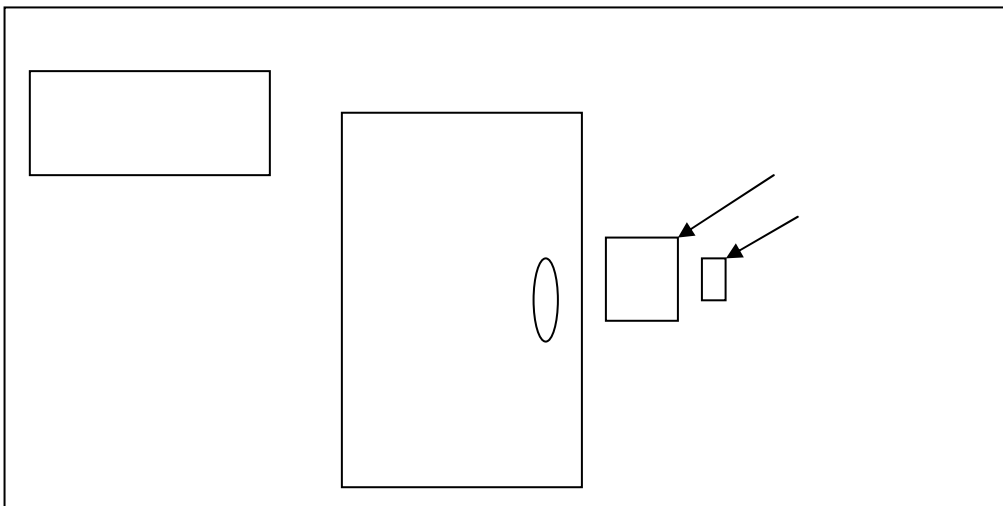
Outside Wiegand Module: ONLY RF <- **enhance security and record all the IN/OUT event.**



Example 3

(Without built-in RF module, External Wiegand reader only) <- *set the Wiegand Input as “Out Door Read Card” mode*

External Wiegand reader: Following the User Access Method (FP only, RF only, RF + FP, RF+ FP+ PIN etc.)



Summary

- If you connect with Built-in RF Module only, follow the User Access Method you have preset.
- If you connect external reader only, follow the User Access Method you have preset.
- If you connect with both Built-in RF Module and External Reader, the Built-in RF Module will follow the User Access Method and external Reader must be card only.

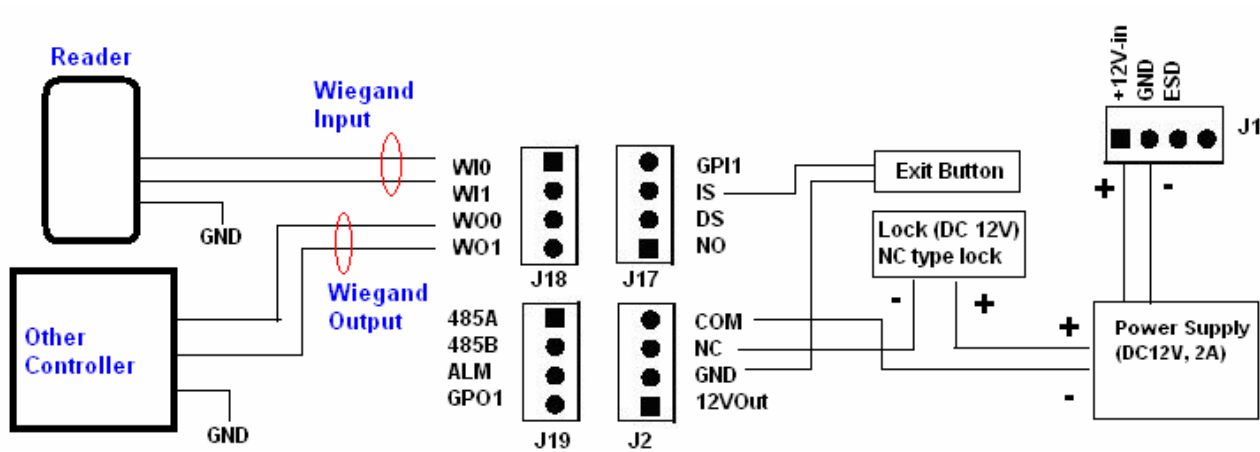
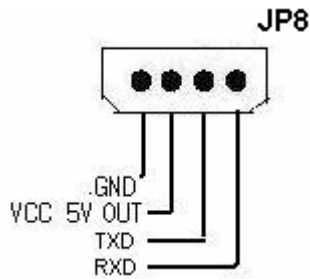


Illustration of i4 Flexi connecting systems

5.6 RF module connection

Mifare standard RF module



RF Module

- 1, 2: Supply VCC 5V to module
- 3: TxD signal
- 4: RxD signal

Communication Format

9600, N, 8, 1

Data storage

Max 8Byte

*Please inform RCG promptly if you plan to use a different module.

5.7 Alarm connection

Type of Alarm provided in i4Flexi

1. Tamper Alarm
2. Forced Open Alarm
3. Alarm Finger
4. General Purpose Input Alarm

Basically, the alarm raised in i4Flexi will trigger a electrical contact output (either Alarm port or General Purpose Output [GPO] port) for connecting external alarm device. E.g. Alarm System, Strobe light, Siren, Buzzer, Alarm Centre and Auto Dialer. *For detail operation, please refer to appendix 1*

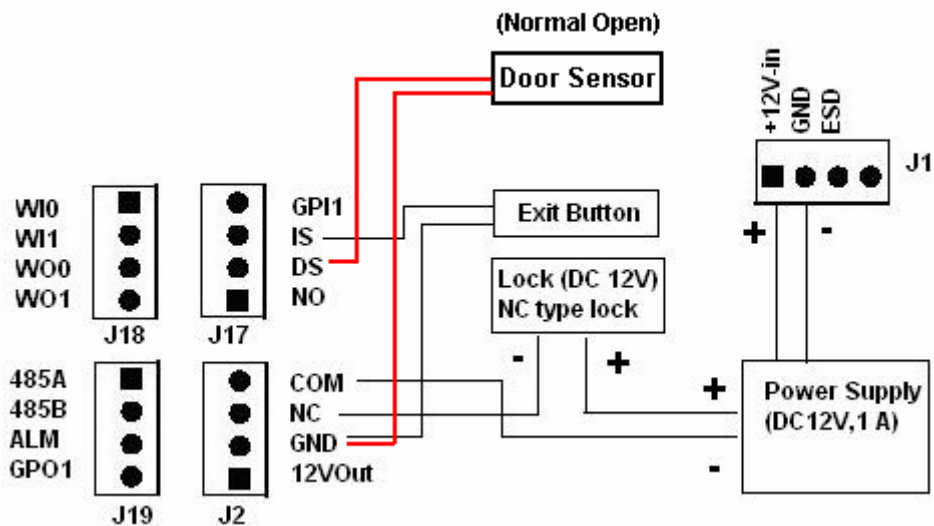


Warning:

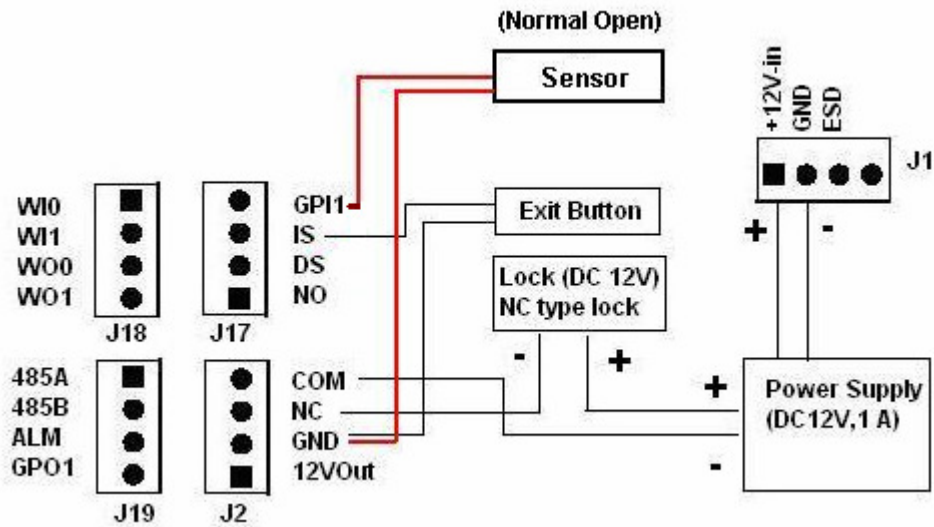
- a. The Alarm / GPO Output port relay is limited max. 3A 120VAC current rating.
- b. The Door Sensor (DS) / General Purpose Input (GPI) port is supposing
 - b. The total current rating is subjected to “Power Supply Rating > total system consumption” but limited less than 3A current. **Failure to do so could result in electric shock leading to serious bodily injury or death.**

Installation of Door Sensor

Controller Connection Diagram for Door Sensor



Controller Connection Diagram for other sensor input (General Purpose Input)



Abbreviation

J2

- 12Vout: 12Volt DC output port
- GND: return circuit port (Ground pin)
- NC: Normal Close (Relay NC pin)
- COM: Common (Relay Com pin)

J17

- NO: Normal Open (Relay NO pin)
- DS: Door Sensor
- IS: Indoor Switch
- GPI1: General Purpose Input 1

J18

- WI0: Wiegand Input Data “0”
- WI1: Wiegand Input Data “1”
- WO0: Wiegand Output Data “0”
- WO1: Wiegand Output Data “1”

J19

- 485A: RS485 A -
- 485B: RS485 B +
- ALM: Alarm Output (Electrical Contact – tight HIGH or LOW is subjected to JP3 setting)
- GPO1: General Purpose Output 1 (Electrical Contact – tight HIGH or LOW is subjected to JP3 setting)

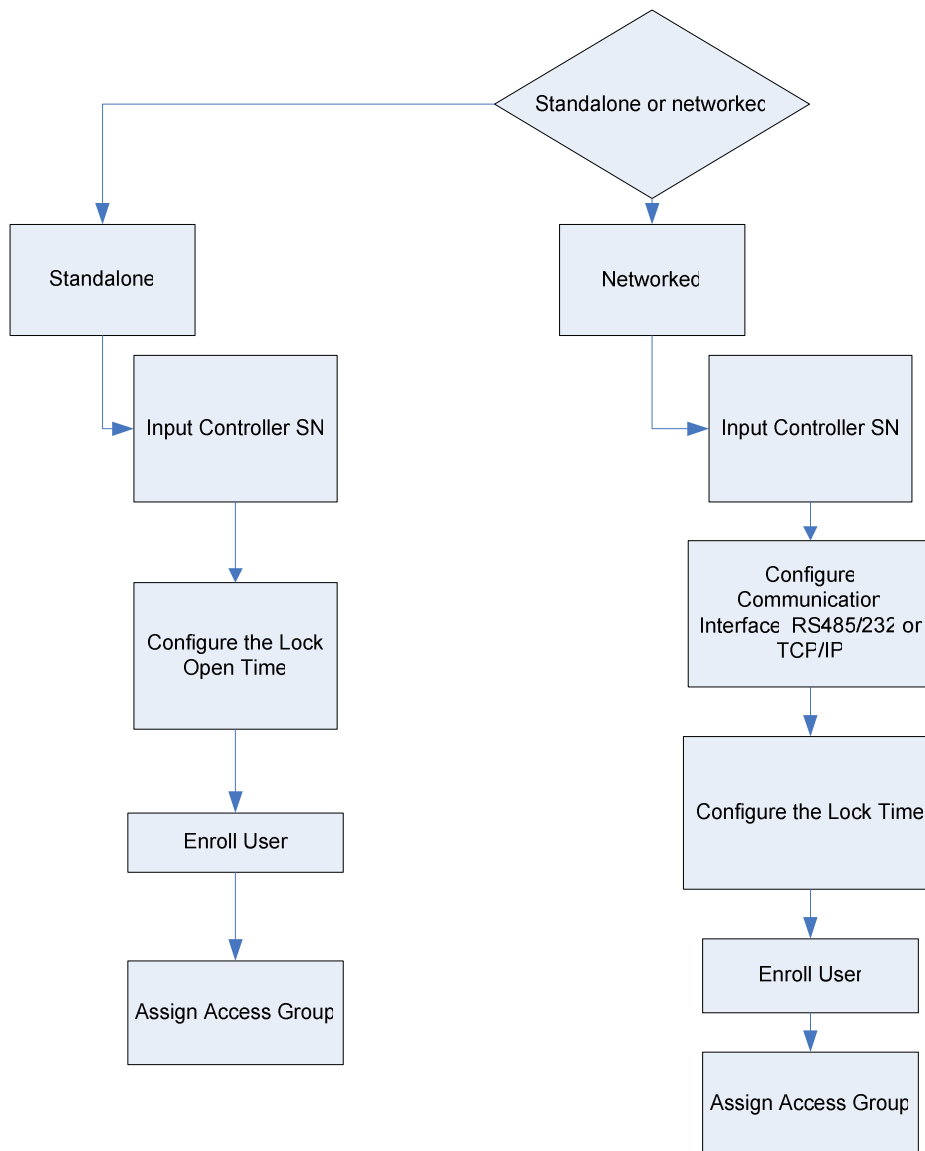
6 Configuration

6.1 Basic Flow

The following section will be conducted when physical installation successfully and system power on.

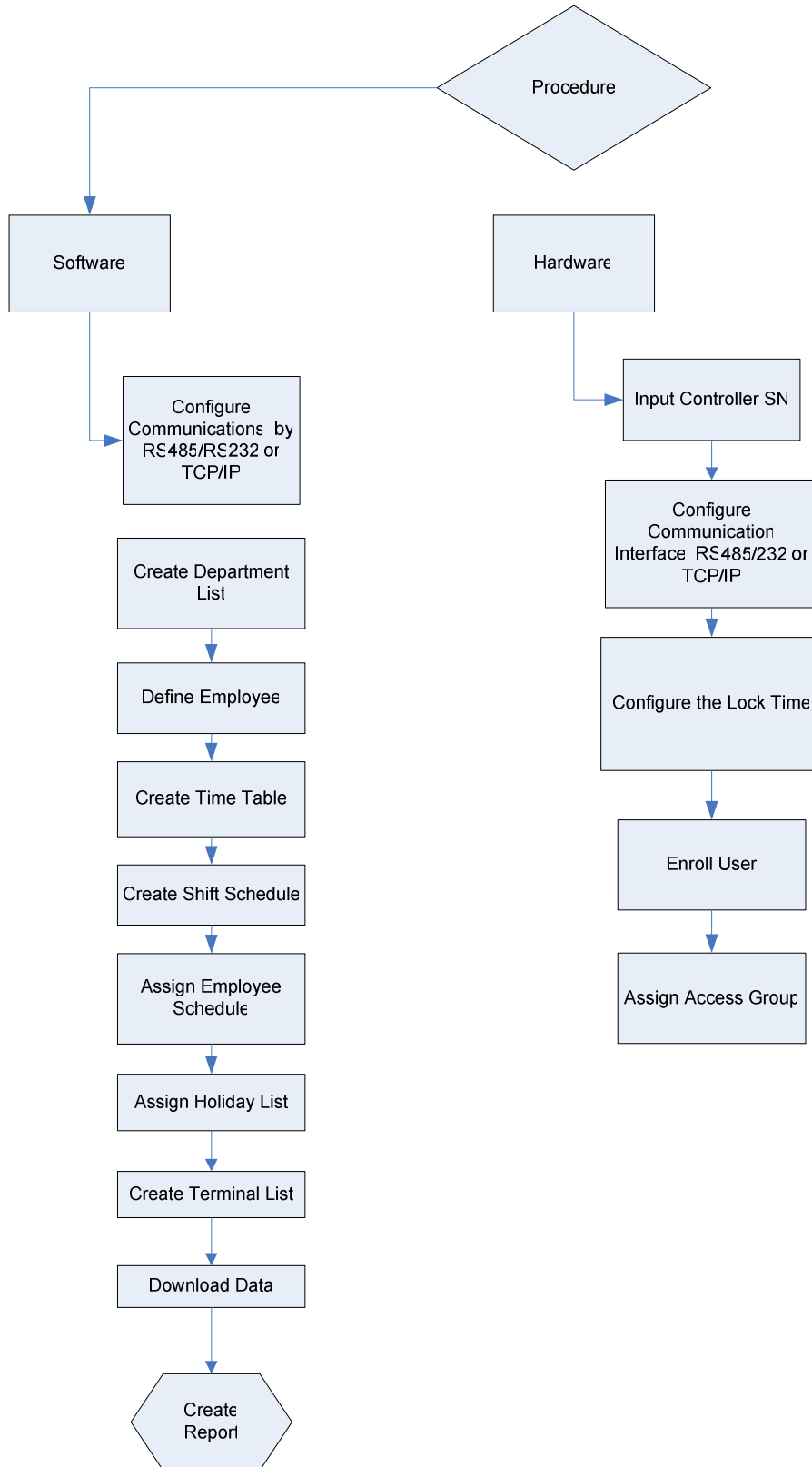
Application for Access Control Configuration

- **Standalone:** The user will operate the i4 Flexi terminal for administration with no data backup capability and the data is stored inside the terminal only.
- **Networked:** The user will connect the i4 Flexi terminal to computer for administration, it is capable to backup the user data, access log and transfer the user data to another new i4 Flexi terminal by using “DAMS” software



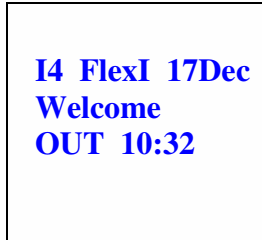
Application for Time Attendance Configuration

- The user will connect the i4 Flexi terminal to computer for administration; it is capable to calculate time attendance by transfer the user data with “DAMS” software.

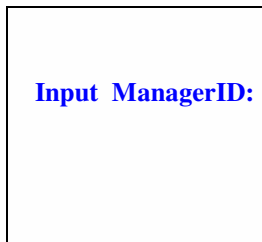


6.2 How to enter the administration menu

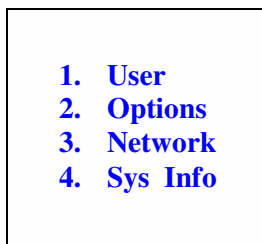
The administrator menu allows new users to register, edit or delete information. Press “Menu”, enter “0” and press “#” to access the administrator mode and then enter ‘1111’ as the initial password.



The standby screen as show here.



1. Press “Menu” key,



2. Enter ID “0” and then follow with “#” to confirm and enter “1111” as the initial password.

6.3 Network

For i4 Flexi, “Ethernet, RS485” and “Wiegand Input or Output” is simultaneous. However, Ethernet and RS485 are alternatives. If the Ethernet is used, RS485 cannot be used. Likewise, if the RS485 is used, the Ethernet cannot be used.

Terminal ID: The machine number ranges from 1 to 999

Baud rate: The communication speed of the communication with the computer at 19200.

Device IP address: The default IP is 192.168.0.201. You may modify it according to your requirements.

Subnet Mask: The default subnet mask is 255.255.255.0,

Gateway: The default gateway is 192.168.0.200

Host IP: The host computer IP to manage the terminal. You may modify it according to your requirements.

Host Port: The default port number is 8008. Except for special circumstances, this number should not be changed.

Mac Address: Display the MAC address.

Network speed: The default network speed is 10M, 100M or AUTO detect.

COMM Key: The System default keyword is none, which is optional to be modified. COM Key is a security code when communicate with PC software. Connection established when COM key matched.

Wiegand Output: To assign the Wiegand output type: 26 bit or 34 bit or disable

Wiegand Input: To assign the Wiegand input mode: Out Door Card or In Door Card

Wiegand Content: to assign the Wiegand data content: Card Number or User ID.

⚠ **Warning:** *When RS485 communication used in the outdoor environment, the lightning protection device needs to be installed.*

6.3.1 Terminal ID

To operate terminals in the network users must first choose an ID. Users can select “3.System=>2.Terminal ID=> new TID“ for as many as 999 terminals and then choose “MENU“ to store data.

The following steps show how to enter network option page

<u>LCD Display</u>	<u>Description</u>
1. User 2. Options 3. Network 4. Sys Info	In the standby mode, press the [MENU] key to enter the Setup menu.
1. Terminal 2. Controller 3. Network Mode	1. Press “3” to enter Network page. (A function to set the networking option)
Terminal ID ID (1-999): 123	2. Press “1” key or select the item with “#” key to enter.
	3. Input the terminal ID and press “#” to save and return to previous menu.

6.3.2 Controller SN

To access the Controller SN registration function on the LCD window, go to the stage “3.Network=>2 Controller , => input serial number of controller” and set details.

To activate other communication functions, the main unit sends a register command to the controller. This only needs to be done once for each unit-controller pair. If either the main unit or the controller has been replaced, an error will occur during communications. In such instances, registration should be repeated.

A relay function inside the controller manages the Ethernet cable. During initialization, the Ethernet cable is disconnected, but it becomes connected after registration of the main unit.

The following steps show how to register controller serial number into terminal

<u>LCD Display</u>	<u>Description</u>
<p>1. User 2. Options 3. Network 4. Svs Info</p>	<p>In the standby mode, press the [MENU] key to enter the Setup menu.</p> <p>1. Press “3” to enter Network page. (A function to set the networking option)</p>
<p>1. Terminal ID 2. Controller 3. Network Mode</p>	<p>2. Press “2” key or select the item with “#” key to enter. .</p>
<p>ID:</p> <p>14600003</p>	<p>3. Input the serial number of controller and press “#” to save and return to previous menu.</p> <p>➡ Note: The controller serial number is 8 digit number and the label stick at the bottom of controller unit.</p>

6.3.3 Network Mode

The Network mode option is a function to set the event log output to network or to Wiegand. Also, it is a function to assign the network parameter. In addition, it is an operation mode with “Wiegand” setting:

6.3.3.1 TCP/IP

Select these methods when you use the Internet to access the terminal. Follow the process “3.Network =>3.Network Mode=>2.TCP/IP“, press “#” to enter the setup menu.

The following steps show how to register TCP/IP parameter

LCD Display	Description
<p>1. User 2. Options 3. Network 4. Sys Info</p>	<p>In the standby mode, press the [MENU] key to enter the Setup menu.</p>
<p>1. Terminal 2. Controller 3. Network Mode</p>	<p>1. Press “3” to enter Network page. (A function to set the networking option)</p>
<p>1. Wiegand Output 2. TCP/IP 3. Com Key 4. WiegContent 5. WiegandInput</p>	<p>2. Press “3” key or select the item with “#” key to enter.</p>
<p>1. Device IP 2. Subnet Mask 3. Gateway 4. Host IP 5. Host Port 6. MAC Address</p>	<p>3. Press “2” key or select the item with “#” key to enter. The following interface appears</p>
<p>IP: 192.168.000.234</p>	<p>4. Press the key number or select the item with “#” key to enter the setting menu of each function.</p> <p>➡ Note: Press “#” key to save and return to previous menu after each setting modified.</p>
	<p>5. For example, to modify the device IP, the following interface appears</p>
	<p>➡ Note: Use “Up” or “Down” key to select the portion and enter the number.</p>

6.4 User Registration

6.4.1 How to register user

Press “menu”, “0” and “#” to input ‘1111’ as the initial password.

First, follow the process “1.User => 1.Add User” and “Add User ID:” appears on screen.

If the ID entered is already in use, “User Exist” will appear on screen.

(Maximum number of digit is 8)

How to add new user

I4 FlexI 17Dec
Welcome
OUT 10:32

1. Press “Menu” key, enter “0” and then follow with “#” to confirm and enter “1111” as the initial password.

1. User
2. Options
3. Network
4. Sys Info

2. Select “1. user”

1. Add User
2. Modify User
3. Delete User

3. Select “1.Add user”

Add User ID
█

4. An “Add User ID” message prompt appears. You are required to input the user ID

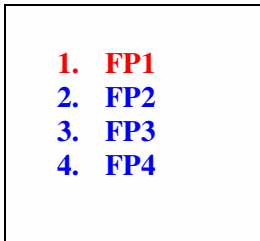
1. User Type
2. Access Mode
3. FP
4. Password
5. Card
6. User Associate
7. FP level

5. Enter “Add user ” page.

6.4.2 Fingerprint registration

To register a fingerprint, place your finger on the red light sensor after pressing “3. FP” in the “Add user” page (see above). Registration is complete after you register with one of the access factor and press “Esc”. The system will then automatically move to the upper menu. To increase authentication rate or register additional fingers, press “2. FP2” and follow the same process required in “1. FP” registration.

.▣ The asterisk (*) appears on the right side of the menu when you save.



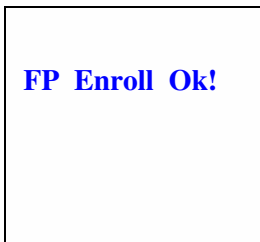
1. After pressing “3. FP”, FP 1 – 8 is normal finger, FP 9-10 is alarm finger.
Select FP ID and place finger on red light sensor



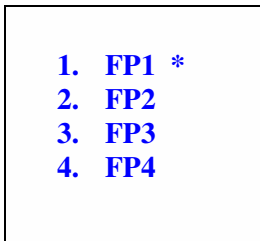
2. Place finger on red light sensor



3. Place finger on red light sensor one more time



4. Enroll FP ok. The screen will return to FP page.



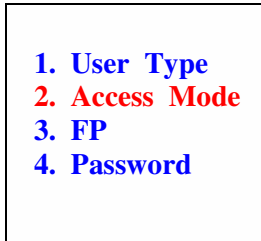
5. The asterisk (*)besides “FP1” indicates successful fingerprint registration

Notes 1: Repeat step 1- 4 for another finger

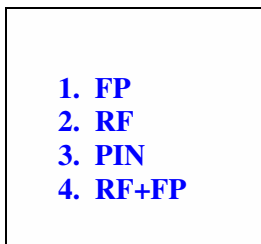
Notes 2: After FP enrollment, a successful registration will be done after access mode assigned – follows section 6.2.6

6.4.3 Activate FP, Card, Password Access Mode

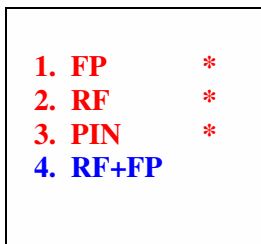
To authenticate an FP, PIN or RF card, follow the process “2. Access Mode=>1. FP, 2. Card & 3. PIN” with the tick mark (*) by pressing “#” or a corresponding number. Press “Esc” to save and return to the upper menu.



1. Select “2.Access Mode”



2. Select item number to activate the corresponding mode e.g. Press “1. FP, 2. RF & 3.PIN” access mode This makes access mode by either one of the selection.



3. Press “Esc” to save and return to the upper menu

6.5 Use & Authentication method
Place your finger on the sensor.

<p>I4 FlexI 17Dec Welcome OUT 10:32</p>	<p>1. Standby screen</p>
<p>Finger * Card Password</p>	<p>2. Place your registered finger on the sensor or input your ID & press “#”.</p>
<p>Finger Capturing..</p>	<p>3. A progress screen “Finger Capturing” appear</p>
<p>Processing..</p>	<p>4. A progress screen “ Processing..”appear</p>
<p>Verify OK 1</p>	<p>3. A message appears to indicate your fingerprint has been recognized and your identification verified</p>
<p>Verify Fail</p>	<p>4. A message shows failure to verify your identification</p>

If authentication fails, please repeat the process.

6.6 System with Wiegand Connection

6.6.1 Wiegand Content

The Wiegand content is a function to select the data content for 1. Card Number, 2. User ID. This enables the Wiegand output data content as card number or user ID, depends on real situation or application.

The following steps show how to select the Wiegand content parameter

<u>LCD Display</u>	<u>Description</u>
<ol style="list-style-type: none"> 1. User 2. Options 3. Network 4. Svs Info 	<p>In the standby mode, press the [MENU] key to enter the Setup menu.</p> <ol style="list-style-type: none"> 1. Press “3” to enter Network page. (A function to set the networking option)
<ol style="list-style-type: none"> 1. Terminal ID 2. Controller 3. Network Mode 	<ol style="list-style-type: none"> 2. Press “3” key or select the item with “#” key to enter.
<ol style="list-style-type: none"> 1. WiegandOutput 2. TCP/IP 3. Com Key 4. WiegContent 5. WiegandInput 	<ol style="list-style-type: none"> 3. Press “4” key or select the item with “#” key to enter.
<ol style="list-style-type: none"> 1. Card 2. User ID 	<ol style="list-style-type: none"> 4. Select the option “1” card data or “2” User ID data. . <p>➡ Note: this enables the Wiegand output data to be card number or user ID.</p>

6.6.2 Wiegand Input

The Wiegand input is a function to build an application with external reader to form a professional access control. For example, some end user would like to change the front end input to be more accuracy data & enhance security. We may plug the i4 flexi with Access method RF+FP as entrance, while plug a RF reader as exit.

The following steps show how to select the Wiegand input mode

<u>LCD Display</u>	<u>Description</u>
<ol style="list-style-type: none"> 1. User 2. Options 3. Network 4. Svs Info 	<p>In the standby mode, press the [MENU] key to enter the Setup menu.</p> <ol style="list-style-type: none"> 1. Press “3” to enter Network page. (A function to set the networking option)
<ol style="list-style-type: none"> 1. Terminal ID 2. Controller 3. Network Mode 	<ol style="list-style-type: none"> 2. Press “3” key or select the item with “#” key to enter.
<ol style="list-style-type: none"> 1. WiegandOutput 2. TCP/IP 3. Com Key 4. WiegContent 5. WiegandInput 	<ol style="list-style-type: none"> 3. Press “5” key or select the item with “#” key to enter.
<ol style="list-style-type: none"> 1. OutDoorRCard 2. InDoorRCard * 	<ol style="list-style-type: none"> 4. Select the option “1” or “2” for the application installed. <p>➡ Note: this enables the Wiegand Input mode to be “Out Door Read Card” or “In Door Read Card”. (see example 2 or 3 as mentioned above)</p>

6.6.3 Wiegand Output

The Wiegand output is a function to export transaction in real time to other access controller following the Wiegand standard 26 bit or 34 bit. When this is enabled, there should be another access controller connected with i4 Flexi 's controller via Wiegand connection. It is the easier way to replace the existing card system but remains the aged controller as reporter and compatible aged HR software.

The following steps show how to select the Wiegand Output mode

<u>LCD Display</u>	<u>Description</u>
<ol style="list-style-type: none"> 1. User 2. Options 3. Network 4. Svs Info 	<p>In the standby mode, press the [MENU] key to enter the Setup menu.</p> <ol style="list-style-type: none"> 1. Press “3” to enter Network page. (A function to set the networking option)
<ol style="list-style-type: none"> 1. Terminal 2. Controller 3. Network Mode 	<ol style="list-style-type: none"> 2. Press “3” key or select the item with “#” key to enter.
<ol style="list-style-type: none"> 1. WiegandOutput 2. TCP/IP 3. Com Key 4. WiegContent 5. WiegandInput 	<ol style="list-style-type: none"> 3. Press “1” key or select the item with “#” key to enter.
<ol style="list-style-type: none"> 1. 26 Wiegand 2. 34 Wiegand 3. Disable * 	<ol style="list-style-type: none"> 4. Select the option “1” or “2” or “3” for the application installed. <p>➡ Note: this enables the Wiegand Output mode to be “26 bit wiegand output ” or “ 34 bit wiegand output” or disabled.</p>

7 Tips and precautions

7.1 First setting in initial use

- Change system password to ensure security
- “1111” as the default setting password
- Power up the device after cabling work is completed

7.2 Difficult fingerprints

- Remove dirt, ensure fingers are dry and try again
- Maintain finger on sensor for more than one second without moving finger

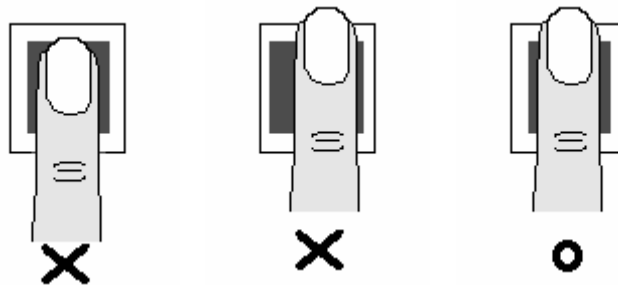
7.3 Reset i4 Flexi and return to setting status before last trial

- When i4 Flexi malfunctions without an apparent problem, press the Reset switch to return to setting status before the last trial.
- Contact the i4 Flexi customer support center for assistance

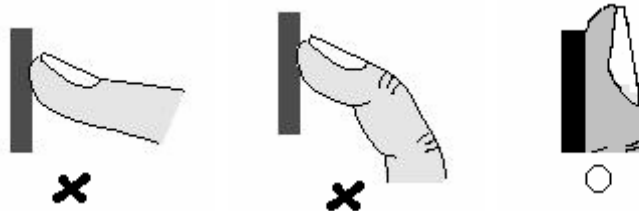
7.4 Right fingerprint registration position



- Correct fingerprint registration position placement
- **During registration**, a quality score will appear for every finger press. For the *mark below 60*, it is recommend to re-registration or use other finger to obtain the better score.



- Correct fingerprint touching placement.



7.5 Cleaning the Sensor

Depending on the amount of use, the sensor window may need to be cleaned periodically.

To clean it, apply the sticky side of a piece of adhesive cellophane tape on the window and peel it away.



Under heavy usage, the window coating on some sensors may turn cloudy from the salt in perspiration. In this case, gently wipe the window with a cloth (not paper) dampened with a mild ammonia-based glass cleaner.

7.6 Sensor Maintenance Warnings

There are several things you should never do when cleaning or using the sensor

- Do not pour the glass cleaner directly on the sensor window.
- Do not use alcohol-based cleaners.
- Never submerge the sensor in liquid.
- Never rub the window with an abrasive material, including paper.
- Do not poke the window coating with your fingernail or any item, such as a pen.

8 Appendix 1 – i4Flexi Alarm Operation

Type of Alarm provided in i4Flexi

1. Tamper Alarm
2. Forced Open Alarm
3. Alarm Finger
4. General Purpose Input Alarm

Type	Response Port	Reset Method	Remark
Tamper Alarm	ALARM	Authorized User Verified by any method	Built in
Forced Open Alarm	GPO	Authorized User Verified by any method	Sensor required
Alarm Finger	ALARM	Authorized User Verified by any method	Default feature
GPI Alarm	GPO	Authorized User Verified by any method	Sensor required

Basically, the alarm raised in i4Flexi will trigger a electrical contact output (either Alarm port or General Purpose Output [GPO] port) for connecting external alarm device. E.g. Siren, Buzzer, Alarm Centre, Auto Dialer.

Example of Alarm

Tamper Alarm

Prize open the i4Flexi Main Unit shell. The Alarm relay is turn ON in the controller alarm port. This port is electrical contact which providing tight high (12VDC) logic or tight Low (GND) logic in the port <Depends on jumper setting>.

Forced Open Alarm

The “Alarm for Invalid Door Opening” is applied in the system parameters; an alarm will be triggered in the event the user pushes the door open to enter without system verification. The GPO relay is turn ON in the controller GPO port. This port is electrical contact which providing tight high (12VDC) logic or tight Low (GND) logic in the port. <Depends on jumper setting>.

Alarm Finger

The “Alarm Finger” is applied in the system parameters. The fingerprint detected by the system for fingerprint verification upon door opening will be the registered alarm finger verified. The GPO relay is turn ON in the controller GPO port. This port is electrical contact which providing tight high (12VDC) logic or tight Low (GND) logic in the port. <Depends on jumper setting>.

General Purpose Input Alarm

The “Alarm for GPI” is applied in the system parameters; an alarm will be triggered in the event the user pushes the sensor (Motion detector, Door Sensor, Output of other device). The GPO relay is turn ON in the controller GPO port. This port is electrical contact which providing tight high (12VDC) logic or tight Low (GND) logic in the port. <Depends on jumper setting>.

Alarm Operation

1. Tamper Alarm

When i4Flexi casing is prizing, it will case the case sensor to turn ON and activate the “tamper alarm” and turns ON corresponding device to operate if any.



Tamper Alarm => make controller “ALM” port” ON => electrical contact ON

Notes: **RESET ALARM: *If the shell is closed properly. The alarm will be off.*

2. Forced Open Alarm



Caution: To enable this feature, a “*Normal Open Door Sensor (Dry Contact)*” is required.

The “Alarm for Invalid Door Opening” is applied in the system parameters; an alarm will be triggered in the event the user pushes the door open to enter without fingerprint verification.



Notes: **RESET ALARM: Verification of any authorized finger.

3. Alarm Finger

When user the registered alarm finger. System will assume the user is under highjack. GPO port will be trigger.



Caution: To enable the feature, you must *enroll alarm finger* into device.

Notes: **RESET ALARM: Verification of any authorized finger.

4. General Purpose Input Alarm



Caution: To enable this feature, a “*Normal Open Sensor (Dry Contact)*” is required.

The “Alarm for General Purpose Input” is applied in the system parameters; an alarm will be triggered in the event the user pushes the sensor.



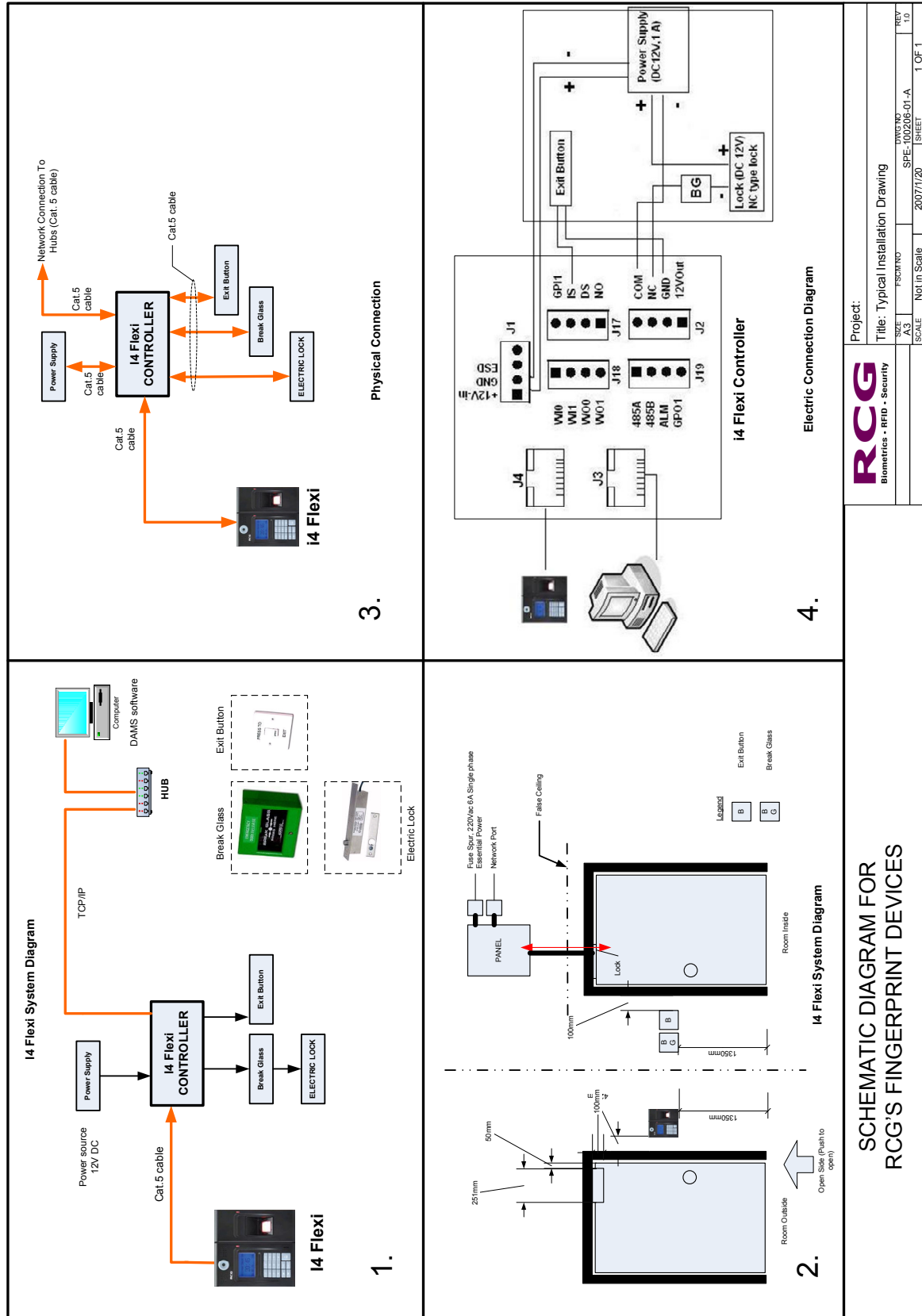
Notes: **RESET ALARM: Verification of any authorized finger.

Indicator Light

There are three indicator lights in the Controller:

	Red Light	Yellow Light	Green Light
Lock Control Unit	Power Connected	Light blinking while traffic with processor	Unlock legally

9 Appendix 2 – Quick Start Procedure & Drawing



Project:		Title: Typical Installation Drawing	
SCALE	Proj No	REV	NO
Not in Scale	2007/1/20	SPE-100206-01-A	1.0
SHEET		1 OF 1	

RCG	
Biometrics • RFID • Security	

Step By Step Work Flow

System Configuration

- 1 Connect the system as shown in "Installation Drawing"
- 2 Check connection
- 3 Power On the system

Step 1

Procedure to activate the device

- 1 Press: "Menu", "0", "#", "1111" to enter the main menu on device
- 2 Press: "3", "2", Key in the SN of controller e.g. "14600001", "#"
- 3 Done!

(refer to manual section 11.1.2)

Remarks 1: Controller SN must be key in to main unit as this will disable all the function if it is not matched

Step 2

Procedure to enroll fingerprint

- 1 Follow the manual section 6.2.2 "How to register"

Step 3

Procedure to link up PC

- 1 Follow the manual section 11.1.1 "Terminal Registration"
- 2 set Terminal ID
- 3 set Device IP
- 4 set Server IP

Step 4

Procedure to use the software

- 1 Follow with the manual, "i4. i4+ S903 i4Flexi Installation Guide 1130"
- 2 install and setup the connection

Step 5

Procedure to operate DAMS & Device

- 1 Add Company
- 2 Add Department
- 3 Add Duty Group
- 4 Add Timeable
- 5 Add Employee
- 6 Add Duty Group per employee

Step 6

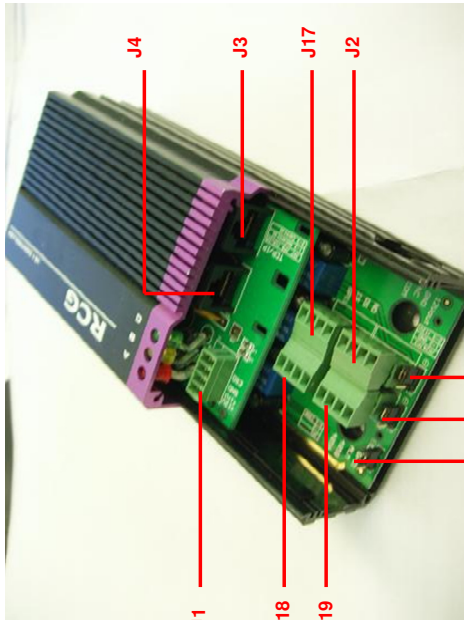
Procedure to transfer template

- 1 Follow the quick reference guide for detail

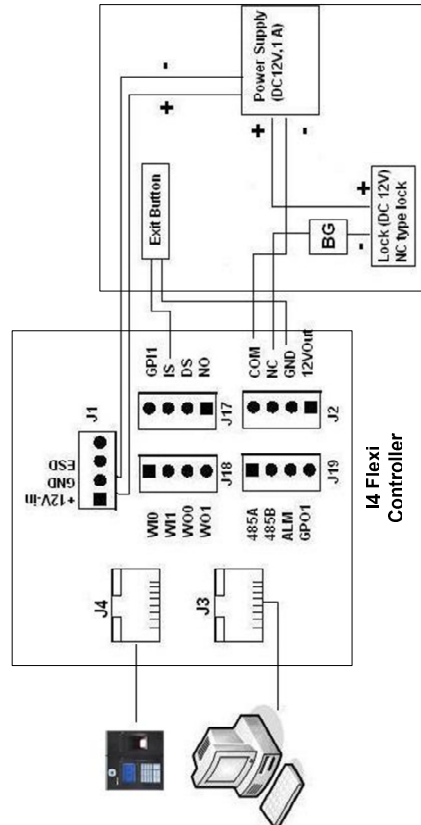
Step 7

Generate Report

- 1 follow with DAMS user manual



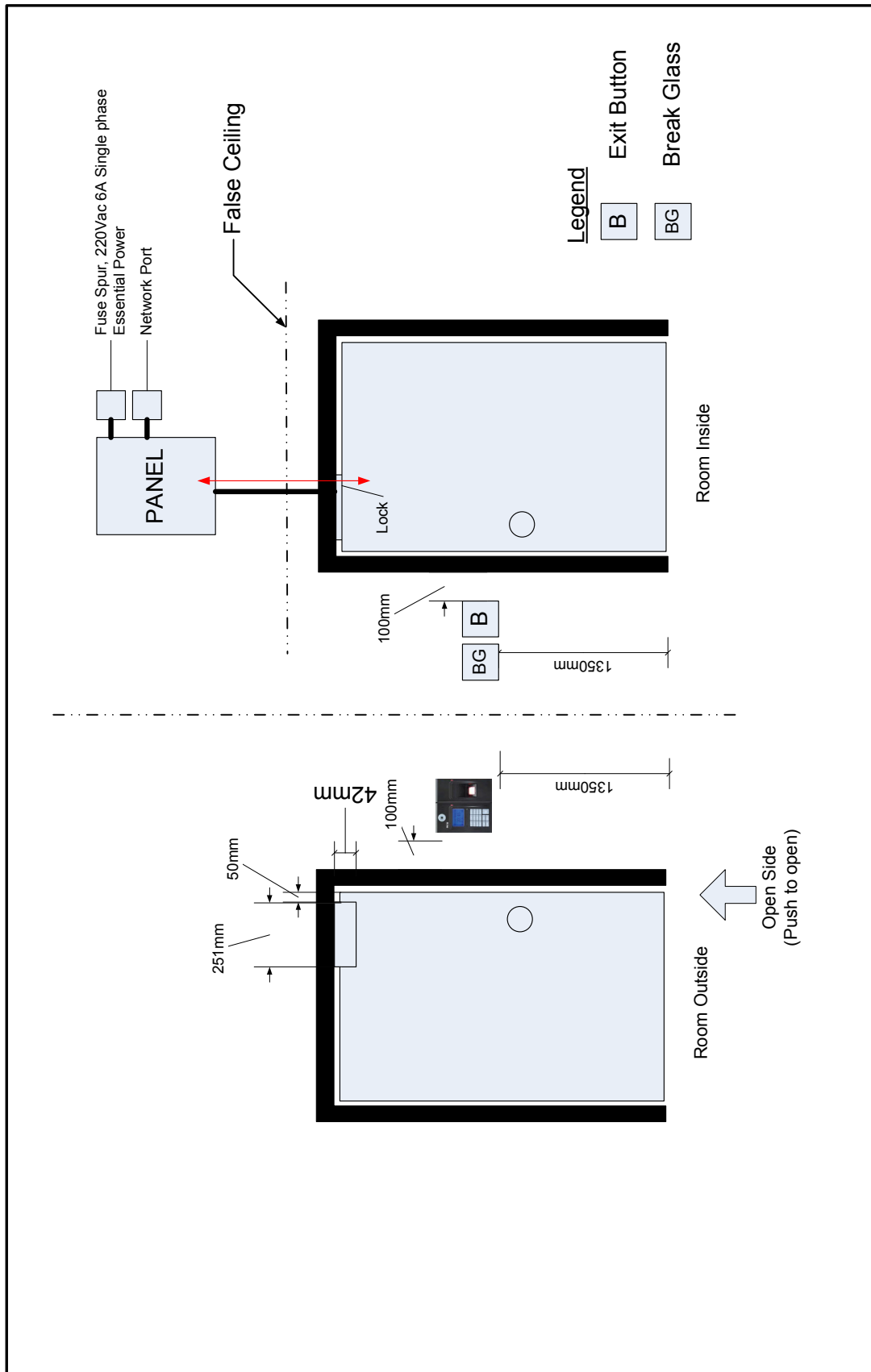
J1 JP1 JP2 JP3



SCHEMATIC DIAGRAM FOR RCG'S FINGERPRINT DEVICES

Project:		Title: Typical Installation Drawing	
SCALE	Not in Scale	DATE	2007/1/20
NO.	A3	REVISED BY	SPE 100206.02 A
SHEET		1 OF 1	

RCG	
Biometrics • RFID • Security	



		Project:	
		Title: Typical Installation Drawing for EM Lock	
SIZE: A3	PROJECT NO: SPFE-100206-03-A	DATE: 2007/1/20	REV: 1.0
SCALE: Not In Scale	SHEET: 1	TOF I	

Typical Installation Drawing for EM Lock

10 Glossary

User: type of user

Alarm Finger: a finger is defined as special function

Normal Door Open: Authorized verification to open the door

Invalid Door Open: Any door opening action other than Normal door opening

Card, Fingerprint and password verification: authentication mode

Finger relevancy: User security level

FRR: ‘False Rejection Rate’

FAR: “False Acceptance Rate”

DC: Direct Current

GND: -ve or return path, called Ground

Tx: Transmit

Rx :Receive

GPI: General Purpose Input

GPO: General Purpose Output

NO: Normal Open

NC: Normal Close

DS: Door Status

IS: Indoor Switch, (Exit button)

FP: Fingerprint

RF: Radio Frequency Card

PIN: Password

11 Support Information

Web Site	http://www.rcg.tv/support/
Hotline Support	Hong Kong : 852-36696999 Malaysia : +6-03-51248888 Customer Service is available : Monday to Friday 9:00 am – 6:00 pm(local time)
Support Email	support@rcg.tv