

Security Expert

Security Purpose Door Control Unit

Installation Manual

May 2023

Legal Information

The Schneider Electric brand and any registered trademarks of Schneider Electric Industries SAS referred to in this manual are the sole property of Schneider Electric SA and its subsidiaries. They may not be used for any purpose without the owner's permission, given in writing. This manual and its content are protected, within the meaning of the French intellectual property code (Code de la propriété intellectuelle français, referred to hereafter as "the Code"), under the laws of copyright covering texts, drawings and models, as well as by trademark law. You agree not to reproduce, other than for your own personal, noncommercial use as defined in the Code, all or part of this manual on any medium whatsoever without Schneider Electric's permission, given in writing. You also agree not to establish any hypertext links to this manual or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the manual or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

Electrical equipment should be installed, operated, serviced and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

As standards, specifications and designs change from time to time, please ask for confirmation of the information given in this publication.

Trademarks and registered trademarks are the property of their respective owners.

Contents

Introduction	5
Installation Requirements	6
Grounding Requirements	7
Safety Grounding	7
Earth Ground Connection	7
Mounting	8
DC Power & Encrypted Module Network	9
End of Line (EOL) Jumper	10
Door Access Control	11
Shield Connection	11
RS-485 Reader Connection	12
RS-485 Reader Connection (Entry/Exit)	13
RS-485 Reader Location	14
OSDP Reader Connection	15
OSDP Reader Location	15
Wiegand Reader Connection	16
Single LED Connection	16
Dual LED Connection	17
Multiple Wiegand Reader Connection	18
Connecting 4 Wiegand Readers	19
Magnetic Reader Connection	20
Door Contact Connection	21
Door Lock Connection	21
Inputs	22
Trouble Inputs	23
Outputs	24
Relay/Lock Outputs	24
Standard Outputs (3 To 8)	24
Beeper Outputs (5 and 8)	25
Address Configuration	26
LED Indicators	27
Status Indicator	27
Fault Indicator	27
Power Indicator	27
Relay Indicators	27
Reader 1/Reader 2 Indicators	28
Input Indicators	28
Error Code Indication	29

Error Code Display	29
Mechanical Diagram	30
Mechanical Layout	31
Technical Specifications	32
New Zealand and Australia	34
European Standards	35
UK Conformity Assessment Mark	38
FCC Compliance Statements	39
Industry Canada Statement	40

Introduction

The Security Purpose Door Control Unit extends the number of card reader connections on the system by 2 (or 4 when using multiple reader mode), the number of inputs by 8 (four inputs used for door monitoring and control, and up to eight for extended functionality), and the number of outputs by 12 (includes 6 relay lock control outputs).

Flexible module network architecture allows large numbers of modules to be connected to the RS-485 module network, over a distance of up to 900M (3000ft). Further span can be achieved with the use of a network repeater module.

The current features of the door control unit include:

- Standard mode, allowing connection of 2 Wiegand readers controlling 1 door (entry and exit) or 2 doors (entry or exit only)
- Multiplex mode, allowing connection of 4 Wiegand readers (connected in multiplex mode) controlling 2 doors (entry and exit)
- Standard RS-485 Reader mode for up to 4 RS-485 capable readers (2 per port) providing either entry/exit on 2 doors or a combination of entry or exit on up to 2 doors
- RS-485 reader port connections support configuration for OSDP protocol
- Offline functions including All Users, First 10 Users plus 150 Card Cache, and No Users
- Secure encrypted RS-485 module communications
- 8 inputs
- 6 lock Form C relay outputs
- 6 open collector outputs (reader control outputs)
- Krone type (IDC) link connectors (screw terminals for main 24V DC input connection)
- Cross connection terminal block - additional terminal block for 16 pairs of free connections (1 Krone and 1 screw terminal per pair)
- Smart reader missing/tamper monitoring
- Easy mounting in Schneider Electric DCU 605 plastic enclosure (provided)
- Online and remote upgradeable firmware

Installation Requirements

This equipment is to be installed in accordance with:

- The product installation instructions
- The Local Authority Having Jurisdiction (AHJ)

Grounding Requirements

An effectively grounded product is one that is *intentionally connected to earth ground through a ground connection or connections of sufficiently low impedance and having sufficient current-carrying capacity to prevent elevated voltages which may result in undue hazard to connected equipment or to persons.*

Grounding of the Security Expert system is done for three basic reasons:

1. Safety
2. Component protection
3. Noise reduction

Safety Grounding

The object of safety grounding is to ensure that all metalwork is at the same ground (or earth) potential. Impedance between the Security Expert system and the building scheme ground must conform to the requirements of national and local industrial safety regulations or electrical codes. These will vary based on country, type of distribution system and other factors. The integrity of all ground connections should be checked periodically.

General safety dictates that all metal parts are connected to earth with separate copper wire or wires of the appropriate gauge.

Earth Ground Connection

The door control unit must be grounded to a suitable single-point earth ground connection in the installation. A minimum 14AWG solid copper wire (or thicker, in accordance with local authorities) shall be used from the Security Expert system's earth connection points.

There must be only **one** single earth grounding point per system.

Mounting

The door control unit is designed to mount directly into the Schneider Electric DCU605 plastic enclosure.

It is recommended that the enclosure is installed:

- On a straight wall or in a ceiling above the corridor in a safe sheltered space
- On a wall near doors
- Over a recessed installation box

Ensure the door control unit is always installed on the safe side of a door.

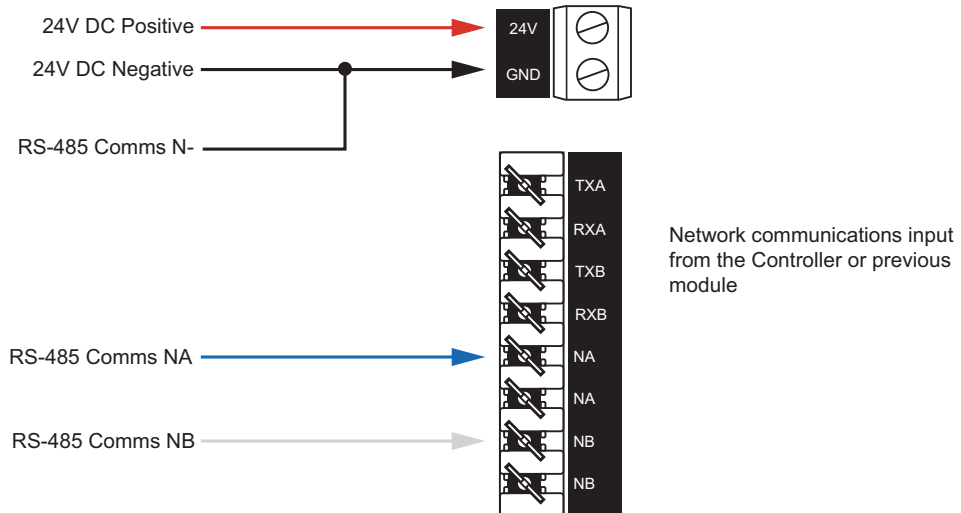
Mounting the Door Control Unit

1. Select mounting knockouts to be removed from the plastic enclosure.
2. Determine which cables will be routed into the housing and insert these through the plastic cable inlets.
3. Position the rear of the plastic enclosure against the wall and mark the location of the mounting holes.
4. Mount the housing to the wall using mounting screws. Ensure that the screw heads **do not** touch the bottom of the PCB.
5. Insert the door control unit into the plastic enclosure and secure with fastening screws.

DC Power & Encrypted Module Network

The Security Purpose Door Control Unit should be powered using 24VDC connected to the 24V and GND terminals.

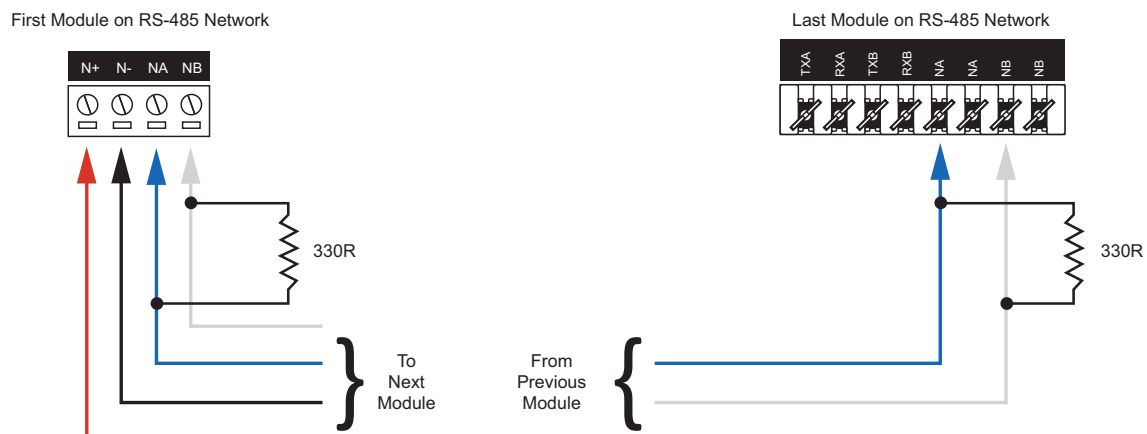
Connection of the communications and DC supply should be performed according to the diagram shown below.



Warning:

- The Module 24V input must be supplied from only *ONE* point. Connections from more than one 24V supply may cause failure or damage to the door control unit or device supplying module power to any door control unit.
- It is important that the network communications power be 12VDC supplied from an independent battery backed power supply unit capable of supplying the required voltage to all devices on the RS-485 network.
- It is important to ensure that all network communication ground connections are connected between all module devices and door control units.
- The door control unit should not be used to supply the 12VDC network communications power. However, the RS-485 network N- should be connected as shown above.

End of Line Resistors



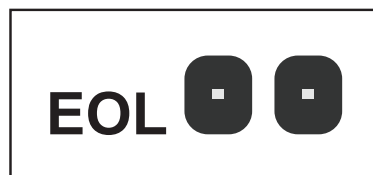
End of Line (EOL) Jumper

When the door control unit is located at the start or end of the module network, the end of line (EOL) jumper should be **on** in lieu of the standard 330 ohm resistor across the NA and NB terminals.

EOL Jumper On



EOL Jumper Off



Door Access Control

The Security Purpose Door Control Unit allows the connection of up to 4 reading devices controlling 2 doors with entry and exit readers.

Each reader port can be independently configured to support one of the following protocols:

- Schneider Electric RS-485 (Schneider Electric readers only)
- OSDP (Open Supervised Device Protocol)
- Wiegand

Recommended Cabling

The recommended cable types for RS-485 are:

- Belden 9842 or equivalent
- 24 AWG twisted pair with characteristic impedance of 120ohm

Maximum distance: 900m (3000ft)

The recommended cable types for Wiegand are:

- 22 AWG alpha 5196, 5198, 18 AWG alpha 5386, 5388

Maximum distance: 150m (492ft)

Shield Connection

Important:

- The card reader must be connected to the module port using a shielded cable.
- The shield must only be connected at one end of the cable in the metallic enclosure (frame grounded).
- Do not connect the cable shield to an AUX-, 0V or V- connection on the module.
- Do not connect the cable shield to any shield used for isolated communication.
- The reader pigtail shield and cable shield wires should be joined at the reader pigtail splice.
- Do not terminate the reader shield wire inside the reader.

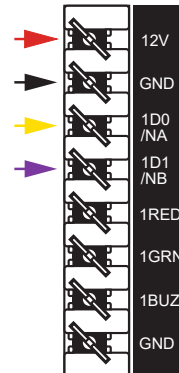
Always refer to the card reader manufacturer for detailed installation guidelines.

RS-485 Reader Connection

Security Expert readers can be connected in RS-485 configuration. The following shows the connection of a single RS-485 reader for entry only.

Third-party RS-485 readers can only be connected using the OSDP protocol (see page 15).

Reader Port Connections



Reader Wiring Connections

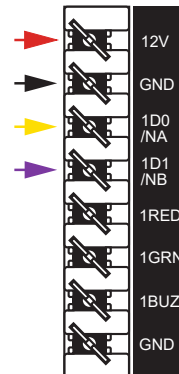
The reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	12V 12VDC positive
12VDC- negative	GND 12VDC negative
RS-485 A	D0/NA RS-485 A
RS-485 B	D1/NB RS-485 B
Shield (drain)	Frame grounded at one point only

RS-485 Reader Connection (Entry/Exit)

The following shows the connection of two RS-485 readers to provide an entry/exit configuration.

Reader Port Connections



Primary Reader Wiring Connections

The primary reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	12V 12VDC positive
12VDC- negative	GND 12VDC negative
RS-485 A	D0/NA RS-485 A
RS-485 B	D1/NB RS-485 B
Shield (drain)	Join the shield (drain) wires together. Frame grounded at one point only

Secondary Reader Wiring Connections

The secondary reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	Join to primary reader 12VDC+ positive wire
12VDC- negative	Join to primary reader 12VDC- negative wire
RS-485 A	Join to primary reader RS-485 A wire
RS-485 B	Join to primary reader RS-485 B wire
Shield (drain)	Join the shield (drain) wires together. Frame grounded at one point only

RS-485 Reader Location

As two RS-485 readers can be connected to the same reader port, the reader **address** uniquely identifies each reader and determines which is the entry reader and which is the exit reader.

Configuration	Location
Reader address = 0	Entry
Reader address = 1	Exit

All Schneider Electric readers use address 0 (entry) by default, unless configured otherwise. The reader's address can be configured by applying the required reader address TLV setting to the reader programming.

For programming instructions, see the *Security Expert Card Reader Configuration Guide*.

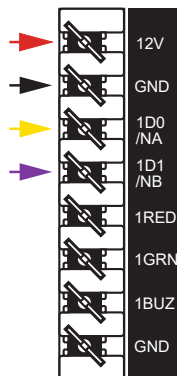
SX readers are hardwired to use address 1 when the reader's **green** and **orange** wires are joined together. For more information, see the SX reader installation manual.

OSDP Reader Connection

When using the OSDP protocol the reader is connected to the reader port using a standard RS-485 wiring configuration. The following shows the connection of a single OSDP reader for entry only.

Connection of two OSDP readers to provide an entry/exit configuration follows the same connection requirements as connecting two RS-485 readers (see page 13).

Reader Port Connections



This connection example shows wiring for Security Expert readers. Other readers may use different color configurations. Always refer to the card reader manufacturer for detailed installation guidelines, and see the table below.

Reader Wiring Connections

The reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	12V 12VDC positive
12VDC- negative	GND 12VDC negative
RS-485 A	D0/NA RS-485 A
RS-485 B	D1/NB RS-485 B
Shield (drain)	Frame grounded at one point only

Connecting OSDP readers requires additional hardware configuration and system programming. For more information, see *Application Note 254: Configuring OSDP Readers in Security Expert*.

For more information about OSDP support on Security Expert card readers, including configuring readers for secure channel communications, see *Application Note 321: Configuring Security Expert Readers for OSDP Communication*.

OSDP Reader Location

As two OSDP readers can be connected to the same Security Expert module reader port, each OSDP reader is configured as either an *Entry* or *Exit* reader in the **Reader location** setting of the associated **smart reader** record.

OSDP reader location is **not** determined by the reader address.

Wiegand Reader Connection

When connecting a reader to a Security Expert reader expander using the Wiegand interface, the reader can be wired in either single LED configuration.

Only card readers with two Wiegand LED lines support dual LED operation.

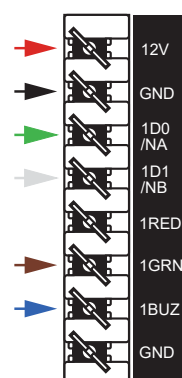
Single LED Connection

Single LED operation is the standard Wiegand configuration and allows a single LED line to control the two reader LEDs. This results in two possible LED states: color 1 or color 2.

All Security Expert readers are shipped to operate in single LED mode by default.

The following shows the wiring configuration of a Wiegand reader for entry only, using single LED operation.

Reader Port Connections



This connection example shows wiring for Security Expert readers. Other readers may use different color configurations. Always refer to the card reader manufacturer for detailed installation guidelines, and see the table below.

Reader Wiring Connections

The reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	12V 12VDC positive
12VDC- negative	GND 12VDC negative
Wiegand Data 0	D0/NA Wiegand Data 0
Wiegand Data 1	D1/NB Wiegand Data 1
Wiegand LED control	GRN Wiegand LED control
Wiegand beeper control	BUZ Wiegand beeper control
Shield (drain)	Frame grounded at one point only

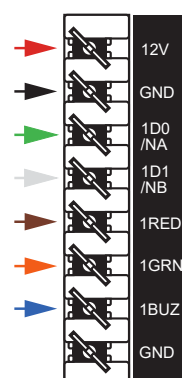
Dual LED Connection

Dual LED operation uses two LED lines to independently control the two LEDs. This results in four possible LED states: color 1, color 2, both colors on (produces a third, combined color), or both colors off. The additional states may be used to show the status of alarms or other integrated signals.

The reader must support dual LED operation. Security Expert SX readers support this functionality, however the reader needs to be programmed to operate in dual LED mode. For programming instructions, see the *Security Expert Card Reader Configuration Guide*.

The following shows the wiring configuration of a Wiegand reader for entry only, using dual LED operation.

Reader Port Connections



This connection example shows wiring for Security Expert readers. Other readers may use different color configurations. Always refer to the card reader manufacturer for detailed installation guidelines, and see the table below.

Reader Wiring Connections

The reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	12V 12VDC positive
12VDC- negative	GND 12VDC negative
Wiegand Data 0	D0/NA Wiegand Data 0
Wiegand Data 1	D1/NB Wiegand Data 1
Wiegand LED 2 control	RED Wiegand LED control
Wiegand LED 1 control	GRN Wiegand LED control
Wiegand beeper control	BUZ Wiegand beeper control
Shield (drain)	Frame grounded at one point only

Multiple Wiegand Reader Connection

In multiple reader mode, the secondary card reader has all connections wired to the same reader port as the primary reader, except the Data 1 connection which is wired to the Data 1 input on the alternate reader port.

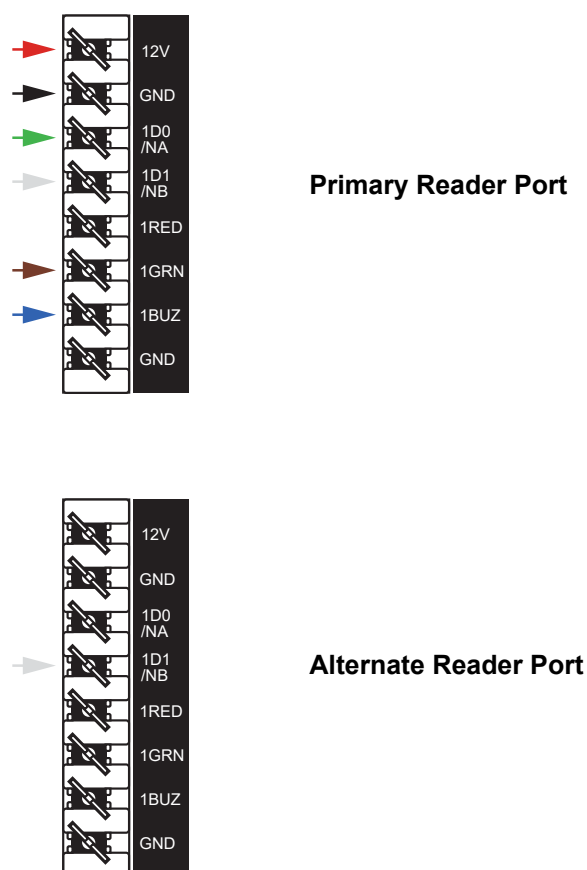
The normal primary reader connection operates as the **entry** reader, and the secondary reader that is multiplexed into the alternate reader port will operate as the **exit** reader.

To connect two Wiegand readers to a reader port the **Multiple reader input port 1/2** option must be enabled in the reader expander programming. When this option is disabled the reader port will only process a single reader.

The following shows the connection of two Wiegand readers to provide an entry/exit configuration.

Reader Port Connections

This example assumes the standard single LED configuration. For dual LED operation connect the primary reader port as described in the previous topic.



This connection example shows wiring for Security Expert readers. Other readers may use different color configurations. Always refer to the card reader manufacturer for detailed installation guidelines, and see the table below.

Entry Reader Wiring Connections

The entry reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	12V 12VDC positive
12VDC- negative	GND 12VDC negative
Wiegand Data 0	D0/NA Wiegand Data 0
Wiegand Data 1	D1/NB Wiegand Data 1
Wiegand LED control	GRN Wiegand LED control
Wiegand beeper control	BUZ Wiegand beeper control
Shield (drain)	Join the shield (drain) wires together. Frame grounded at one point only

Exit Reader Wiring Connections

The exit reader should be connected using the wiring configuration outlined in the table below.

Reader Wire	Connection
12VDC+ positive	Join to entry reader 12VDC+ positive wire
12VDC- negative	Join to entry reader 12VDC- negative wire
Wiegand Data 0	Join to entry reader Wiegand Data 0 wire
Wiegand Data 1	D1/NB Wiegand Data 1 (<i>alternate reader port to entry reader</i>)
Wiegand LED control	Join to entry reader Wiegand LED control wire
Wiegand beeper control	Join to entry reader Wiegand beeper control wire
Shield (drain)	Join the shield (drain) wires together. Frame grounded at one point only

Connecting 4 Wiegand Readers

Multiple reader mode allows the connection of 4 Wiegand readers controlling 2 doors, each with entry and exit readers. To connect 4 Wiegand reading devices:

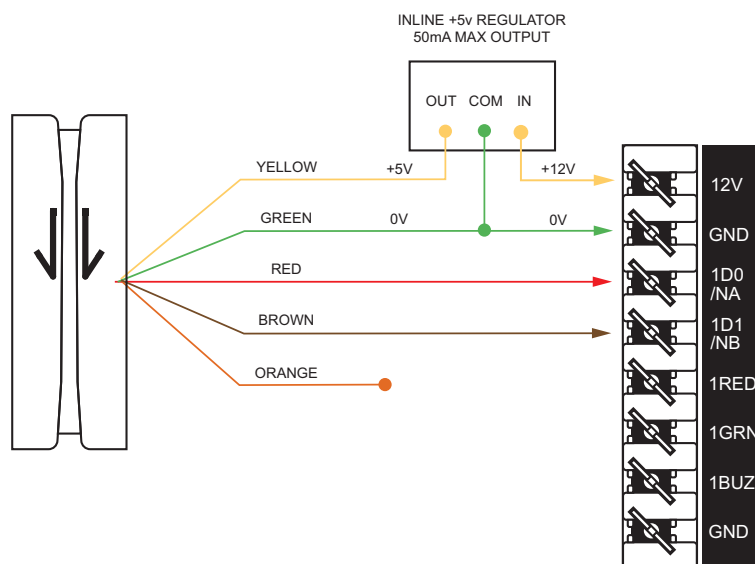
- Door 1 entry reader is connected to reader **port 1**
- Door 1 exit reader has its Wiegand Data 1 wire connected to the reader **port 2** D1 connection
- Door 2 entry reader is connected to reader **port 2**
- Door 2 exit reader has its Wiegand Data 1 wire connected to the reader **port 1** D1 connection
- The **Multiple reader input port 1** option is enabled in the reader expander programming (General | Options)
- The **Multiple reader input port 2** option is enabled in the reader expander programming (General | Options)

To connect two Wiegand readers to a reader port the **Multiple reader input port 1/2** option must be enabled in the reader expander programming. When this option is disabled the reader port will only process a single reader.

Magnetic Reader Connection

The door control unit allows the connection of standard magnetic track 2 format cards and provision is made in the software for a large number of formats. Formats include BIN number for ATM access control and first 4, 5 and 6 card numbers.

Magnetic Card Reader Interface:

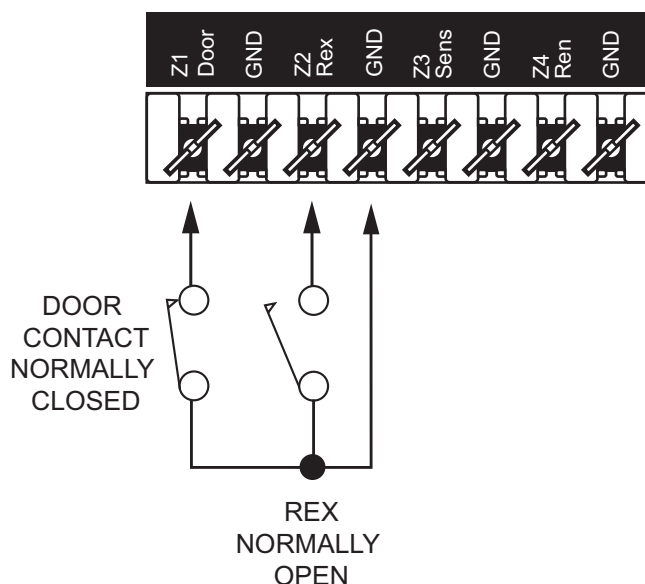


Magnetic card readers are typically operated by 5 volts. Before connecting the magnetic card reader to the reader expander, ensure that the supply voltage is correct and if required insert an inline 5 Volt regulator as shown in the diagram above.

Door Contact Connection

The module allows the connection of up to 4 contacts for monitoring and controlling access control doors. Each input can be used for either the door function that is automatically assigned or as a normal input on the system. The following example shows the connection of a normally closed door position monitoring contact to monitor the open, closed, forced and alarm conditions of the door.

Standard Door Contact Inputs:

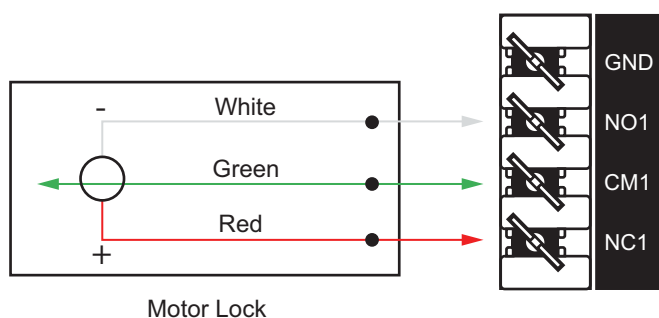


When connected the REX input can be programmed to operate regardless of the door contact state. The REX input can also be programmed to recycle the door alarm time to prevent nuisance alarms when the door is held open to permit longer entry.

Door Lock Connection

The door control unit provides two lock output relays that can be used to switch electric locks.

Door Lock Outputs:



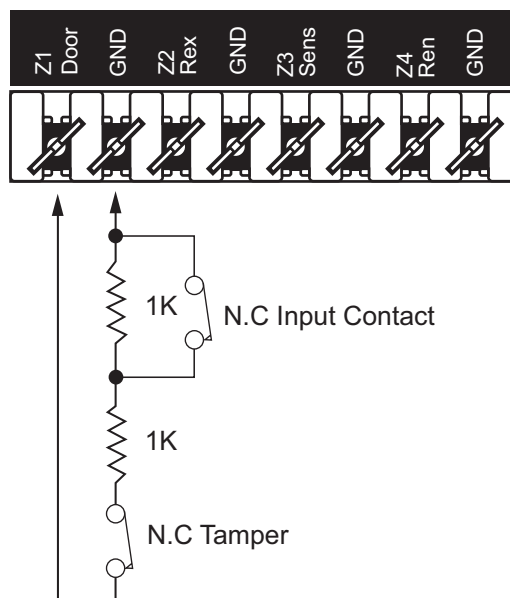
Inputs

The door control unit can monitor the state of up to 8 inputs. These inputs can be connected to a variety of EOL monitored or dry contact devices such as magnetic switches and PIR motion detectors. Devices connected to the inputs can be installed to a maximum distance of 300m (1000ft) from the module when using 22 AWG wire. Each input may be individually configured for normally opened and normally closed configurations with or without EOL resistors for tamper and short condition monitoring.

When using an input with the EOL resistor configuration, the controller generates an alarm condition when the state of an input changes between open and closed and generates a tamper alarm condition when a wire fault (short circuit) or a cut wire (tampered) in the line occurs.

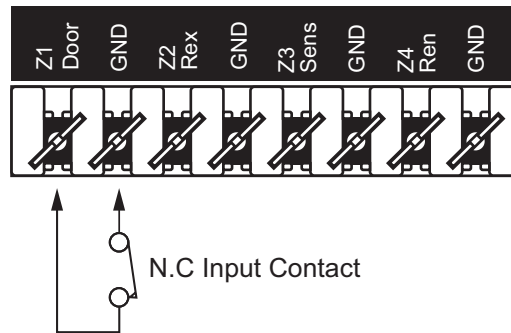
When using the EOL resistor configuration, the EOL resistor option must be enabled in the input programming so that the tamper and short states can be monitored. For more information, refer to your Security Expert programming reference manual.

EOL Resistor Input Configuration:



Each input can use a different input configuration. To program a large number of inputs with the same configuration use the multiple selection feature within the Security Expert software.

When using the 'No Resistor' configuration the controller only monitors the opened and closed state of the connected input device, generating the alarm (open) and restore (closed/sealed) conditions.

No EOL Resistor Input Configuration:

Trouble Inputs

Each door control unit can monitor up to 16 trouble inputs used to report trouble conditions such as module communications problems.

Trouble inputs are used to monitor the module status and in most cases are not physically connected to an external input.

The following table details the trouble inputs that are configured in the system and the trouble groups that they are associated with.

Input Number	Description	Default Trouble Group	Default Trouble Group Option
RDxxx:01	Module Tamper	System	System Tamper
RDxxx:02-05	Reserved	None	None
RDxxx:06	Door 1 Forced	Access	Forced Door
RDxxx:07	Door 2 Forced	Access	Forced Door
RDxxx:08	Door 1 Left Open	Access	Left Open
RDxxx:09	Door 2 Left Open	Access	Left Open
RDxxx:10-11	Reserved	None	None
RDxxx:12	Reader 1 Tamper	System	System Tamper
RDxxx:13	Reader 2 Tamper	System	System Tamper
RDxxx:14	Door 1 Too Many Attempts	Access	Attempts
RDxxx:15	Door 2 Too Many Attempts	Access	Attempts
RDxxx:16	Module Offline	System	Module Offline

Replace 'xxx' with the appropriate address of the module that you are programming.

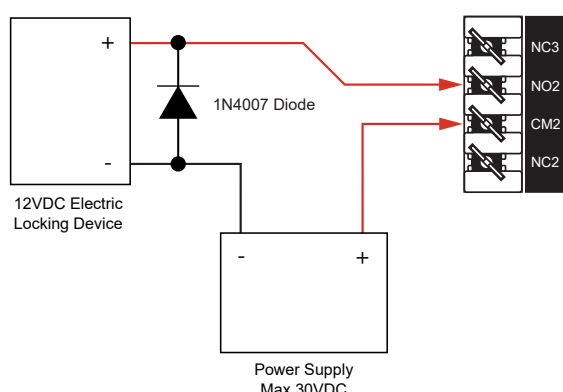
Outputs

The door control unit has 12 programmable outputs. These outputs are used to activate bell sirens, lighting circuits, door locks, relay accessory products and other automation points.

Relay/Lock Outputs

Relays are provided on outputs 1, 2, and 22-25. Relays 1 and 2 are used for the Lock 1 (Output 1 RD001:01) and Lock 2 (Output 2 RD001:02) functions, and are used to control electric door strikes and other lock control devices. Outputs 22-25 control relays 3 to 6. The lock relay will switch a maximum current of 7A resistive or inductive.

Lock Output Connection (Output 2 Shown):



The locking device is connected to the **NO** terminal, as displayed above, for *power to unlock / fail secure* devices. For *power to lock / fail safe* devices the locking device is connected to the **NC** terminal.

The 1N4007 diode is supplied for lock output connections and **must** be installed at the electric strike terminals.

Standard Outputs (3 To 8)

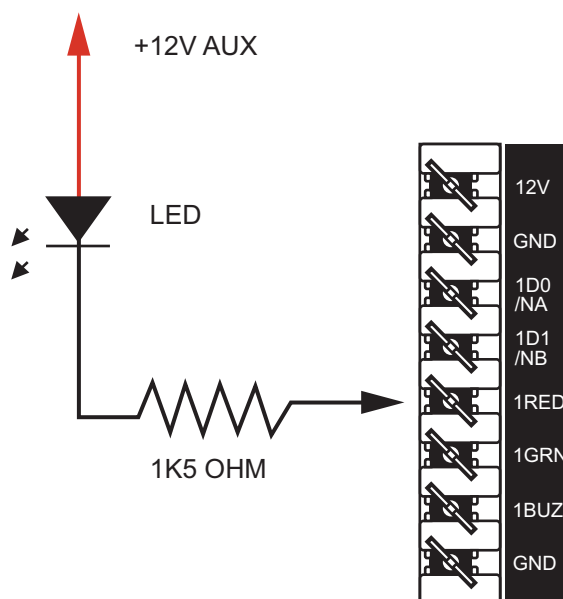
The outputs 3, 4, 5, 6, 7 and 8 on the door control unit are open collector outputs and switch to a ground connection.

The outputs have a default pre-programmed function as detailed in the following table and are used to control the indicator and audible outputs on the attached reading device. These functions may be disabled by programming the appropriate setting in the reader expander configuration.

Output Number	Description
RDxxx:03	LED 1 (Green) Reader 1
RDxxx:04	LED 2 (Red) Reader 1
RDxxx:05	BEEPER Reader 1
RDxxx:06	LED 1 (Green) Reader 2
RDxxx:07	LED 2 (Red) Reader 2
RDxxx:08	BEEPER Reader 2

Replace 'xxx' with the appropriate address of the module that you are programming.

Example Open Collector Output Connection (LED):



Warning: Outputs 3 to 8 can switch to a maximum capacity of 50mA each. Exceeding this amount will damage the output.

Beeper Outputs (5 and 8)

The beeper outputs 5 and 8 on the door control unit provide special diagnostic information when a card is presented. The following table shows the beeper modes of operation.

Function	Description
2 Beeps	Access Granted The lock will activate and allow access to the door at which the card has been presented.
1 Long Beep	Access Denied The card or PIN is not recognized, or the user does not have access to this door.
4 Beeps	Offline Access Granted If the module is operating offline from the controller, the reader generates additional beeps whenever it grants access to a user.

Address Configuration

The module address is configured via programming and will require knowledge of the module serial number. The serial number can be found on the identification sticker on the product.

Refer to the Security Expert system controller configuration guide for address programming details.

The controller has a set limit on the number of modules of each type that it can support. When adding and configuring modules always refer to the *Maximum Module Addresses* table in the controller configuration guide.

LED Indicators

The door control unit includes comprehensive diagnostic indicators that can aid the installer in diagnosing faults and conditions. In some cases an indicator may have multiple meanings depending on the status indicator display at the time.

Status Indicator

The status indicator displays the module status.

State	Description
Fast flash (green)	Module attempting registration with controller
Slow flash (green)	Module successfully registered with controller
Flashing (red)	Module communications activity

When the fault and status indicators are flashing alternately, the module is in identification mode, enabling the installer to easily identify the module in question. Upon either a module update or the identification time period expiring, the module will return to normal operation.

Fault Indicator

The fault indicator is lit any time the module is operating in non-standard mode. If the fault indicator is flashing, the module requires a firmware update or is in firmware update mode. When the fault indicator is on, the status indicator will flash an error code.

State	Description
Continuous slow flash (red)	Module is in boot mode awaiting firmware update
Constantly on (red)	Module is in error state and will flash an error code with the status indicator

Power Indicator

The power indicator is lit whenever the correct module input voltage is applied across the N+ and N- terminals.

State	Description
Constantly on (green)	Correct module input voltage applied
Constantly off	Incorrect module input voltage applied

Relay Indicators

The relay indicators show the status of the lock output relays.

State	Description
Constantly on (red)	Relay output is ON
Constantly off	Relay output is OFF

Reader 1/Reader 2 Indicators

The reader 1 and reader 2 indicators display the status of the data being received by the onboard readers.

State	Description
Short Flash (red)	A short flash (<250 Milliseconds) on the reader 1/reader 2 indicators will show that data was received but was not in the correct format.
Long Flash (red)	A long flash (>1 Second) indicates that the unit has read the data and the format was correct.

Input Indicators

Whenever an input on the module is programmed with an input type and area, the input status will be displayed on the front panel indicator corresponding to the physical input number. This allows for easy test verification of inputs without the need to view the inputs from the keypad or the Security Expert software.

State	Description
Constantly off	Input is not programmed
Constantly on (red)	Input is in an open state
Constantly on (green)	Input is in a closed state
Continuous flash (red)	Input is in a tamper state
Continuous flash (green)	Input is in a short state

Error Code Indication

When the module attempts to register or communicate with the system controller a registration error can be generated indicating that it was not successful.

Error Code Display

The following table is only valid if the **fault** indicator is *constantly on* and the **status** indicator is *flashing red*.

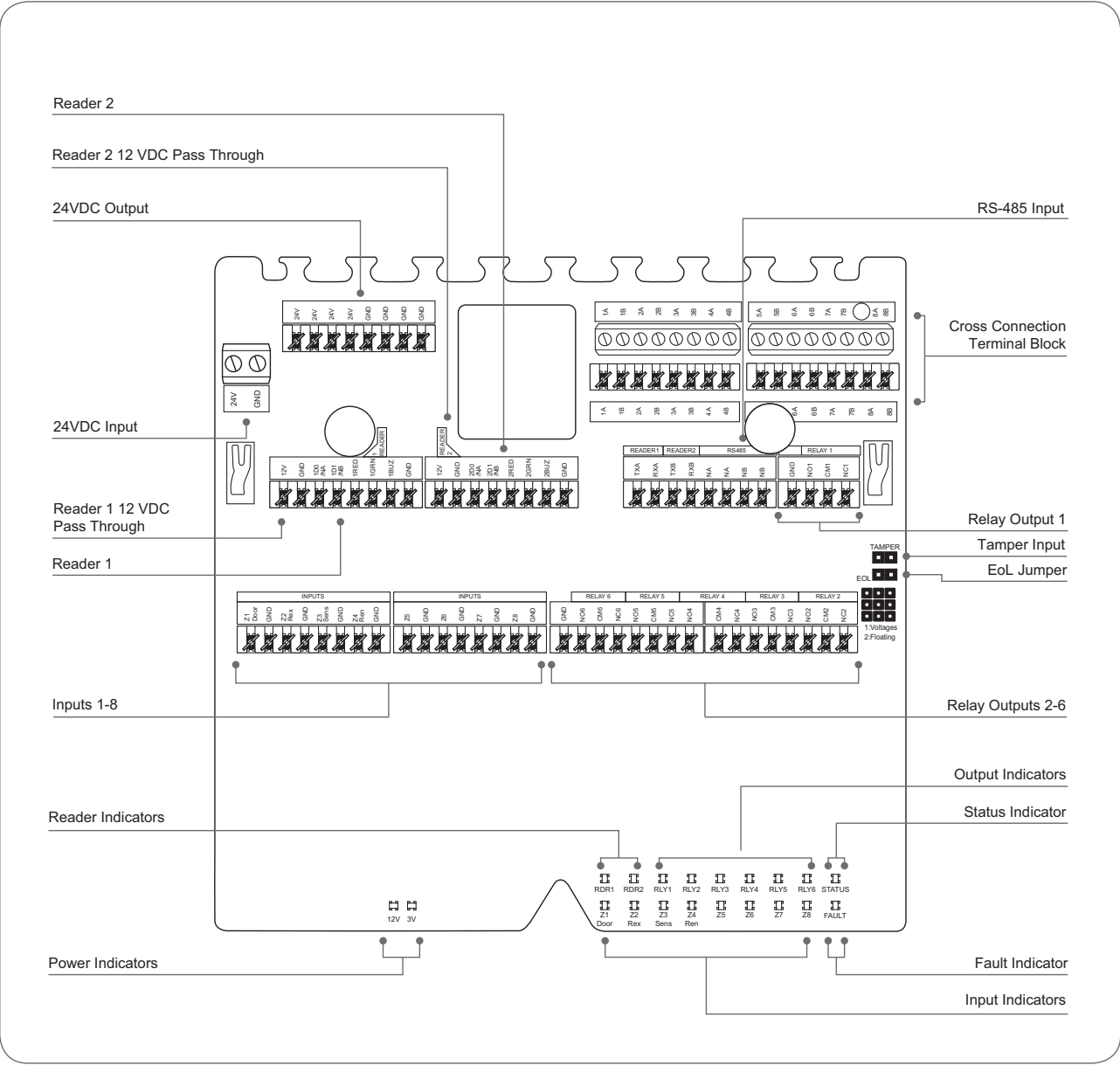
If the fault indicator is *flashing* the module requires a firmware update or is currently in firmware update mode.

The status indicator will *flash red* with the error code number. The error code number is shown with a 250ms on and off period (duty cycle) with a delay of 1.5 seconds between each display cycle.

Flash	Error Description
1	Unknown Error Code The error code returned by the system controller could not be understood by the module.
2	Firmware Version The firmware version on the module is not compatible with the system controller. To clear this error, update the module using the module update feature in the controller's web interface.
3	Address Too High The module address is above the maximum number available on the system controller. To clear this error change the address to one within the range set on the system controller, restart the module by disconnecting the power.
4	Address In Use The address is already in use by another module. To clear this error set the address to one that is not currently occupied. Use the view network status command to list the attached devices, or the network update command to refresh the registered device list.
5	Controller Secured Registration Not Allowed The controller is not accepting any module registrations. To allow module registrations use the network secure command to change the setting to not secured.
6	Serial Number Fault The serial number in the device is not valid. Return the unit to the distributor for replacement.
7	Locked Device The module or system controller is a locked device and cannot communicate on the network. Return the unit to the distributor for replacement.

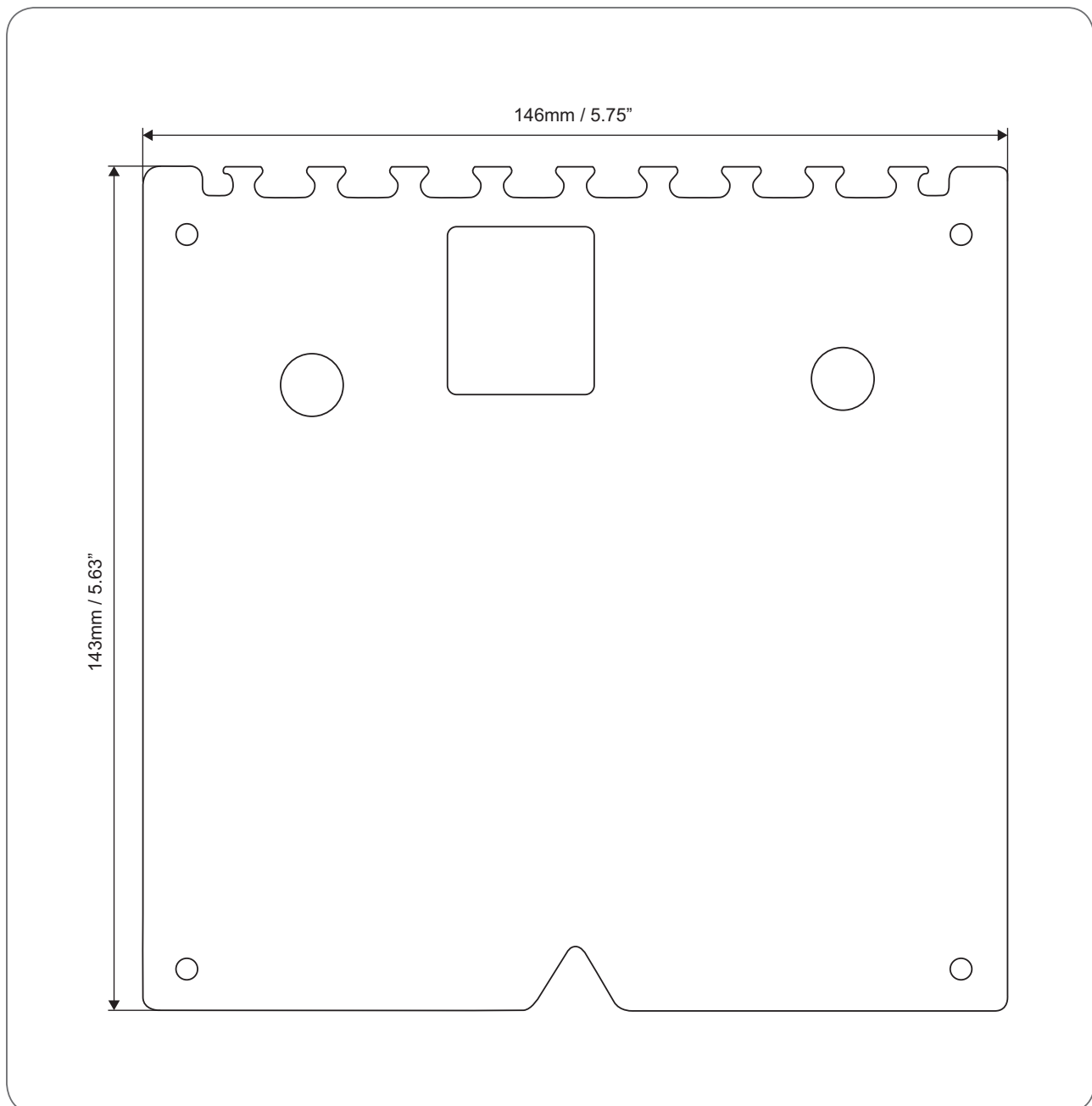
Mechanical Diagram

The diagram shown below outlines the essential details needed to help ensure the correct installation of the door control unit.



Mechanical Layout

The layout shown below outlines the essential details needed to help ensure the correct installation of the door control unit.



Technical Specifications

The following specifications are important and vital to the correct operation of this product. Failure to adhere to the specifications will result in any warranty or guarantee that was provided becoming null and void.

Ordering Information	
SP-DCU	Security Expert Security Purpose Door Control Unit
Power Supply	
DC Input Voltage	20-28VDC
DC Output Voltage (DC IN Pass Through)	20-28VDC Pass Through Reader 1&2 12VDC Pass Through 1.0A (Max)
Operating Current	130mA @24VDC (without external devices) 410mA @24VDC (4 standard Smart Card Readers connected)
Communication	
RS-485	Module network
Offline Operation	
Offline Access Modes	All Users, First 10 Users plus 150 Card Cache, No Users
Readers	
Reader Configurations	2 reader ports, independently configurable for either Wiegand (up to 1024 bits configurable) or RS-485, allowing connection of up to 4 readers providing entry/exit control for two doors **
	RS-485 reader port connections support configuration for OSDP protocol
Outputs	
Lock Outputs	6 Form C Relay Outputs - 7A N.O/N.C. at 30 VAC/DC resistive/inductive (Relay 1 can be configured to provide 24V on output contacts using on-board jumpers)
Programmable Outputs	6 (50mA Max) Open Collector
Inputs	
Inputs	8 High Security Monitored Inputs (10ms to 1hr input speed programmable)
Trouble Inputs	16
Dimensions	
Dimensions (L x W x H)	210 x 160 x 55mm (8.26 x 6.29 x 2.16")
Net Weight	190g (6.7oz)
Gross Weight	Variable packed qty.

Operating Conditions	
Operating Temperature	UL/ULC 0° to 49°C (32° to 120°F) : EU EN -10° to 55°C (14° to 131°F)
Storage Temperature	-10° to 85°C (14° to 185°F)
Humidity	0%-93% non-condensing, indoor use only (relative humidity)
Mean Time Between Failures (MTBF)	622,997 hours (calculated using RFD 2000 (UTE C 80-810) Standard)

The total reader current consumption cannot exceed 1A.

** Each reader port supports either Wiegand or RS-485 reader operation, but *not both at the same time*. If combining reader technologies, they must be connected on separate ports.

It is important that the unit is installed in a dry cool location that is not affected by humidity. Do not locate the unit in air conditioning or a boiler room that can exceed the temperature or humidity specifications.

Schneider Electric continually strives to increase the performance of its products. As a result these specifications may change without notice. We recommend consulting our website (www.schneider-electric.com) for the latest documentation and product information.

New Zealand and Australia

General Product Statement

The RCM compliance label indicates that the supplier of the device asserts that it complies with all applicable standards.



European Standards

CE Statement

Conforms where applicable to European Union (EU) Low Voltage Directive (LVD) 2014/35/EU, Electromagnetic Compatibility (EMC) Directive 2014/30/EU, Radio Equipment Directive (RED) 2014/53/EU and RoHS Recast (RoHS2) Directive: 2011/65/EU + Amendment Directive (EU) 2015/863.

This equipment complies with the rules, of the Official Journal of the European Union, for governing the Self Declaration of the CE Marking for the European Union as specified in the above directive(s).



WEEE

Information on Disposal for Users of Waste Electrical & Electronic Equipment

This symbol on the product(s) and / or accompanying documents means that used electrical and electronic products should not be mixed with general household waste. For proper treatment, recovery and recycling, please take this product(s) to designated collection points where it will be accepted free of charge.

Alternatively, in some countries you may be able to return your products to your local retailer upon purchase of an equivalent new product.

Disposing of this product correctly will help save valuable resources and prevent any potential negative effects on human health and the environment, which could otherwise arise from inappropriate waste handling.

Please contact your local authority for further details of your nearest designated collection point.

Penalties may be applicable for incorrect disposal of this waste, in accordance with your national legislation.

For business users in the European Union

If you wish to discard electrical and electronic equipment, please contact your dealer or supplier for further information.

Information on Disposal in other Countries outside the European Union

This symbol is only valid in the European Union. If you wish to discard this product please contact your local authorities or dealer and ask for the correct method of disposal.

EN50131 Standards

This component meets the requirements and conditions for full compliance with EN50131 series of standards for equipment classification.

EN 50131-1:2006+A2:2017, EN 50131-3:2009, EN 50131-6:2008+A1:2014, EN 50131-10:2014, EN 50136-1:2012, EN 50136-2:2013, EN 60839-11-1:2013

Security Grade 4

Environmental Class II

Equipment Class: Fixed

Readers Environmental Class: IVA, IK07

SP1 (PSTN – voice protocol)

SP2 (PSTN – digital protocol)

SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + PSTN)

SP6 (LAN – Ethernet) and DP1 (LAN – Ethernet + USB-4G modem)

Tests EMC (operational) according to EN 55032:2015

Radiated disturbance EN 55032:2015

Power frequency magnetic field immunity tests (EN 61000-4-8)

EN50131

In order to comply with EN 50131-1 the following points should be noted:

- Ensure for Grade 3 or 4 compliant systems, the minimum PIN length is set for 6 digits.
- To comply with EN 50131-1 Engineer access must first be authorized by a user, therefore Installer codes will only be accepted when the system is unset. If additional restriction is required then Engineer access may be time limited to the first 30 seconds after the system is unset.
- Reporting delay – Violation off the entry path during the entry delay countdown will trigger a warning alarm. The warning alarm should not cause a main alarm signal and is not reported at this time. It can be signaled locally, visually and or by internal siren type. If the area is not disarmed within 30 seconds, the entry delay has expired or another instant input is violated, the main alarm will be triggered and reported.
- To comply with EN 50131-1 neither Internals Only on Part Set Input Alarm nor Internals Only on Part Set Tamper Alarm should be selected.
- To comply with EN 50131-1 Single Button Setting should not be selected.
- To comply with EN 50131-1 only one battery can be connected and monitored per system. If more capacity is required a single larger battery must be used.
- For Security Grade 4 installations, two forms of reporting are required. This can be satisfied using the onboard 2400bps modem included with the modem controller model, or through the incorporation of the SP-4G-USB cellular modem module into the installation with the non-modem controller model.

Anti Masking

To comply with EN 50131-1 Grade 3 or 4 for Anti Masking, detectors with a separate or independent mask signal should be used and the mask output should be connected to another input.

I.e. Use 2 inputs per detector. One input for alarm/tamper and one input for masking.

To comply with EN 50131-1:

- Do not fit more than 10 unpowered detectors per input,
- Do not fit more than one non-latching powered detector per input,
- Do not mix unpowered detectors and non-latching powered detectors on an input.

To comply with EN 50131-1 the Entry Timer should not be programmed to more than 45 seconds.

To comply with EN 50131-1 the Bell Cut-Off Time should be programmed between 02 and 15 minutes.

EN 50131-1 requires that detector activation LEDs shall only be enabled during Walk Test. This is most conveniently achieved by using detectors with a Remote LED Disable input.

To comply with EN 50131-1, EN 60839-11 Security Grade 4 and AS/NZS2201.1 class 4&5 Vibration Detection for PreTamper Alarm, protection is provided by a DSC SS-102 Shockgard Seismic vibration sensor mounted within the system enclosure. Alarm output is provided by a pair of non-latching, N.C. (normally closed) relay contacts, opening for a minimum of 1 second on detection of an alarm connected in series with the 24Hr tamper input (TP) on the PSU (or any other system input designated/programmed as a 24Hr Tamper Alarm).

This relay is normally energized to give fail-safe operation in the event of a power loss. Indication of detection is provided by a LED situated on the front cover. The vibration sensor is fully protected from tampering by a N.C. micro switch operated by removal of the cover.

Enclosure SX-DIN-24 has been tested and certified to EN50131.

By design, all Security Expert EN-DIN-XX DIN Rail Enclosures comply with the EN50131 standards. Tamper protection against removal of the cover as well as removal from mounting is provided by tamper switch.

Warning: Enclosures supplied by 3rd parties may not be EN50131-compliant, and should not be claimed as such.

UK Conformity Assessment Mark

General Product Statement

The UKCA Compliance Label indicates that the supplier of the device asserts that it complies with all applicable standards.



FCC Compliance Statements

FCC Rules and Regulations CFR 47, Part 15, Subpart B

This equipment complies with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules.

Operation is subject to the following two conditions:

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

NOTE: THE GRANTEE IS NOT RESPONSIBLE FOR ANY CHANGES OR MODIFICATIONS NOT EXPRESSLY APPROVED BY THE PARTY RESPONSIBLE FOR COMPLIANCE. SUCH MODIFICATIONS COULD VOID THE USER'S AUTHORITY TO OPERATE THE EQUIPMENT.

Industry Canada Statement

ICES-003

This class A digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

CAN ICES-3 (A)/NMB-3(A)

Schneider Electric

www.schneider-electric.com

© 2023 Schneider Electric. All rights reserved.

May 2023