



SC-06 Stand-Alone Controller with Keypad

Installation and User Manual



Copyright

This Document is Manufacturer's copyright. No part of this Document may be reproduced in any form or by any means without Manufacturer's written permission.

Reservations

Manufacturer bears no warranty related to the content of this Document. Manufacturer reserves the right to revise product documentation and specifications without preliminary notification. Manufacturer bears no responsibility for errors and misprints that may occur in the Document.

Technical specification presented in this Document may differ from the current product version. Please address to **Actec**[®] hardware Vendor for additional information in such a case.

Manufacturer bears no responsibility for complete or partial damage of the hardware related to application of this Document.

Trade Marks

All trade marks of all products mentioned in this Document are the property of Manufacturers.

Contents

Terminology	1
Symbols	1
Technical support	1
1. Introduction	2
Basic Features.....	2
Application	2
Extras	3
2. Performance	4
Access To Premises	4
Lock Control	4
Controller With A Hold Or Security Mode Input.....	4
Controller With RTE Or External Reader	5
3. Engineer and Administrator	6
Engineer Code	6
Administrator Code.....	6
4. Users and their Rights	7
Users Database.....	7
Master Keys	7
5. Controller Factory Settings	8
6. Installation and Connection	9
General Recommendations	9
Design	9
Controller Installation.....	9
Controller Connection	10
Factory Configuration.....	11
Alarm Sensor Mode	12
Additional Reader Mode.....	13
Lock And Alarm Device Digital Control.....	13

7. Controller programming	15
General Information	15
Indication During Programming	15
Symbols	15
Initial Authorization	16
Engineer Code Creation	16
Administrator Code Creation	17
Access Code Change	18
Engineer Code Change	18
Engineer Card Adding/Change	18
Administrator Code Change	19
Administrator Card Adding/Change	19
Controller Configuration (Engineer Commands)	20
Lock Operating Time Setup	20
Lock Type Setup	20
Lock Trigger Mode	21
Trigger mode	21
Lock Digital Control	21
RTE/ER Input Function Programming	22
HLD/SNS Input Programming	22
Access Code Tampering Security	22
Alarm Output Configuration	23
Open Door Time Setup	23
Exit Time Setup	24
Alarm Time Setup	24
Administrator Commands	24
Access Modes Control	25
Users Editing	25
User card adding	25
User Deleting	26
User Group Change	26
Group Code Change	27
Database Clearing	27
User Commands	28
Door Opening	28
Security Mode Enabling	28
Hold Mode Control	29

8. Return to Factory Settings 30

9. Controller Performance 31

 Hold Mode 31

 Security Mode 31

 Alarms 31

 Duress Mode 32

10. Technical Specifications..... 33

11. Complete Delivery and Warranties 34

 Standard Delivery 34

 Extra Hardware..... 34

 Warranties **Error! Bookmark not defined.**

Terminology

Hereinafter there is a list of words and terms important for understanding of access control system performance and programming.

Administrator	Designated user having the right to change the rights of other users.
Database	A special nonvolatile memory of the controller storing data about users keys and codes, as well as their additional rights.
Hold mode	Controller state at which common users are deprived of access. It is enabled with a special switch located inside a room (e.g. on a secretary desk.)
Door Contact	Door state sensor indicating if the door to the premises is currently locked. As a rule it is a hidden sealed contact.
Engineer	In this Document it is a person involved in system installation and setup.
Key	A device for user identification within the system. It may be a plastic no contact (proximity) card or a badge.
Code	Complete term is a Personal Identification Number or a PIN-code. Code is typed on a keypad and is used for user identification within the system.
Security mode	A system state at which the controller watches the door contact sensor (door contact) state or an additional alarm sensor, if the latter is included. In this case common users are deprived of access and any activation of a door contact or alarm sensor initiates alarm.

Symbols

To emphasize specific features related to controller installation, programming and performance they are distinguished with the special symbols:



This sign is used to specify mostly important rules that shall be adhered to in order to avoid bad effect and even controller failure.



This sign is used to mark important recommendations providing for optimum utilization of controller capabilities.



This sign is used to mark useful hints, rules, common terms and definitions.

Technical support

Do not hesitate to address for technical support from a distributor or e-mail your request to the following address:

andy@crow.co.il

1. Introduction

SC-06 is not only a common reader integrated controller, it is a stand-alone access control system of high capability. **SC-06** provides for proximity key and PIN-code access to premises, as well as for premises security mode and special access modes (hold and two-way passage modes, and high security mode insuring key plus code access).

To provide for high immunity the controller has a digital control of the electric lock that makes it impossible to unlock the door even in case when intruder has got to lock control cable (in case of controller outside installation).

On the other hand, reasonable combination of factory settings makes it possible to achieve a simple access control system actually without controller programming that makes controller start-up procedure extremely easy and fast.

Integration of controller, reader and control circuits within one case makes the system design convenient and efficient, as well as the modern elegant style provides for its installation in any office or apartment.

Application of **SC-06** Controller insures access control at various modes as well as organizes premises security without extra costs.

Basic Features

- ❑ The entirely completed stand-alone access control system requiring for a minimum number of external components.
- ❑ Database of up to 512 users capacity capable to assign each user to one of four categories.
- ❑ Three access mode options: key only, key or code, key plus code.
- ❑ Capability of the second external reader connection for a two-way passage, or for higher vandal-proof properties.
- ❑ Entire support of all access control functions: connection of door contact and request to exit button. Door state control.
- ❑ Application of any type of electrically controlled locks. Intruder alarm function along with possible use of additional alarm sensor.
- ❑ Hold function for limitation of access to premises.
- ❑ Lock digital control for higher break-in prevention in case of unauthorized access.

Application

Stand-alone access control system basing on **SC-06** Controller can be used for access control to production and accommodation premises, such as:

- ❑ Small companies offices with up to several hundreds of employees.
- ❑ Apartments and private houses.
- ❑ For control of access to individual rooms and their protection within the building.

Extras

Some extra hardware in addition to the controller is required to install an access control system in an office or a house:

- ❑ Regulated power supply: 12 V output voltage.
- ❑ Electrically controlled lock or latch.
- ❑ It is desirable that the door shall have a door contact and request to exit button. The latter shall provide for a capability to watch door state as well as to control unauthorized door opening.
- ❑ If intruder alarm function will be used, it is necessary to install an infrared, sound or any other alarm sensor having a normally closed contact output.

2. Performance

SC-06 Controller can be flexibly programmed to users' convenience. Below there is a description of peculiar features providing for controller flexibility.

Access To Premises

There are three scenarios of access control programming:

- ❑ Key (card) only.
- ❑ Key or code. If codes are not setup by user, it shall be Mode I. If codes have been setup by user, the controller can be used without cards: as a keypad controller only.
- ❑ Key plus code. This mode requires for presentation of the key with subsequent mandatory code introduction for access to premises. The mode is helpful when a higher level of security is required. In this case both group users codes (one code for a specific category of users), or personal codes may be applied, when each user has a specific code that differs from codes of other users.

Lock Control

Controller supports two lock control modes:

- ❑ Standard mode. In this mode the lock is controlled directly by controller output.
- ❑ Higher security mode. In this mode the lock is controlled with a digital code. Special decoder with an output relay is required for lock connection: it can be supplied as a separate circuit board or included into a special power supply. As a power supply is installed inside guarded premises the door cannot be unlocked by wires connection.

Besides, controller may be programmed for performance with a voltage-opened or voltage-closed lock as well as with a pulse lock (with mechanical relock).

When door contact is installed the controller automatically defines if the door was unlocked and then locked and, if necessary, reduces lock time, if the passage was performed quickly enough.

For impulse locks a door contact installation provides for extra capability to identify the state, when the lock was unlocked and was not reset to a closed state, because the door was not really opened.

Controller With A Hold Or Security Mode Input

One of controller inputs (yellow wire) may change its function with regard to settings introduced by engineer in the course of system installation. Under default (factory) setting this input is purposed for hold switch connection. Yellow wire connection to a common wire transfers controller into a hold mode when users access is impossible without a certain privilege.

In this mode only a door contact input is responded as an alarm source, when security mode is on.

If the function of the input under consideration is reset, it is possible to connect an additional alarm sensor to the controller (such as infrared motion sensor, broken glass

sound sensor, etc.). In this mode the controller watches two inputs, when security mode is enabled:

- ❑ Door contact input.
- ❑ Alarm sensor input.

Alarm output is activated in case of violation at any input. In security mode the users having no privilege to disable the mode will not be able to enter premises.



In circuit with extra alarm sensor the controller provides for a hold mode controllable from a keypad.

Controller With RTE Or External Reader

The door may be opened from the inside with the help of Request to exit button (RTE), or a card (or code), if an external reader is installed.

Controller default settings provide for application of request to exit button connected between a green and black (common) conductors.



The door may be opened from the inside without external reader, however in this case indication of unauthorized access is impossible in operation mode (when controller security mode is not enabled).

With the help of Engineer code controller settings can be changed in such a way that external reader will be connected to a green wire. In this case controller is operated in a mode, which hereinafter will be called a two-way access mode.

In a two-way access mode (with external reader installed) an embedded controller reader is also active and provides for door opening from the inside as well, e.g. if an electromagnetic lock is installed.

If the outside reader (the one installed outside the premises) has to be installed outdoors, and essentially if its vandal-proof properties are of special importance, **SC-04** controller (in reader mode) has to be used.

3. Engineer and Administrator

Engineer Code

New controller shall be installed and programmed to appropriate mode of operation with specific connected hardware. For example, lock time, external reader mode and access mode by key or code shall be setup.

Supplier engineer or a specially trained company expert shall preset these functions. Special code that hereinafter is called an Engineer code, is required for access to configuration functions.



Engineer code is not available in a new controller, so after controller first activation it is necessary to introduce Engineer code to proceed with operations. «Controller Programming» section provides for detailed information on the issue.

Engineer can reset the following controller parameters:

- ❑ To add or change Engineer key.
- ❑ To setup controller configuration: mode of operation, system hardware, lock type, etc.
- ❑ To setup controller functions: lock time, exit time, etc.

Administrator Code

After controller operation mode setup and programming the users shall be entered and removed from controller database (their keys or codes) and other procedures related to current system administration shall be exercised within entire period of controller service life. Administrator code is necessary to insure access to administration functions.

Administrator can reset the following controller parameters:

- ❑ To change Administrator code, to add and change Administrator key (card).
- ❑ To switch controller operation modes: "key only", "key or code", "key plus code".
- ❑ To add, remove and change the rights of system users.

Remember that Engineer and Administrator codes are not available in a new controller, so the first thing to be done after controller first activation or reset of its factory settings is to enter Engineer and Administrator codes. The codes shall be unique.

4. Users and their Rights

Users Database

Controller database is capable to keep up to 512 users. Note that a key, PIN-code and a set of privileges can be provided for each user.

Subject to available key code, PIN-code and privileges, as well as to preset mode of operation the access to premises can be controlled by key, code and key plus code (higher security). The set of privileges provides for each user capability to enable and disable security mode, as well as to have access under hold mode (subject to controller operation mode).

Any user can be assigned to one of four categories (refer to Table below).

Users Categories

User	Access	Access under hold mode	Security mode control	Hold mode control
<i>Common</i>	+	--	--	--
<i>Guard</i>	+	--	+	--
<i>Privileged</i>	+	+	--	--
<i>Master</i>	+	+	+	+

If controller is preset for operation in "PIN only" mode, the users are default depersonalized and use PIN-codes common for a certain category.

Master Keys

Along with data about users the controller may keep Master key codes which provide for programming mode without entering code.

Master keys do not provide for access to premises. Controller memory can keep one Engineer and one Administrator Master key. Master key entry into controller memory does not cancel the possibility to use Engineer and Administrator codes (refer to the above Section).

5. Controller Factory Settings

After controller fabrication as well as after hardware reset it has the following settings:

Lock mode.....	Time controlled
Lock operating time	3 seconds
Lock type	Voltage-opened, without relock
Lock control.....	Direct (without decoder)
Open door time.....	30 seconds
Exit time	0 seconds
Alarm time	0 seconds (by event)
RTE/External reader input mode	By RTE (without external reader)
Hold/Security mode input mode.....	Hold input
Hold in course of access code (key) tampering	Enabled
Alarm output mode	Normally opened (disconnected)
Break-in control at disabled security mode	Enabled
Open door alarm	Disabled
Access code tampering alarm	Disabled
Master keys	Not available
Users.....	Not available
Engineer code	Not available
Administrator code.....	Not available
Common user PIN.....	Not available
Guard PIN	Not available
Privileged user PIN.....	Not available
Master PIN	Not available

6. Installation and Connection

General Recommendations

- ❑ Use only regulated power supply for controller. It is strongly recommended to use power supply with a reserve battery providing for system efficiency (and for capability to unlock the door with code or key) at power supply failure.
- ❑ The length of all connection shall be minimum. It is essential for electrical lock control circuit. Long circuit may cause large voltage drop in electric wiring resulting in lock failures.
- ❑ If the door opens into the street, the controller and power supply shall be desirably located indoors and a vandal-proof reader shall be installed outside.
- ❑ Keep Engineer and Administrator codes in a safe place as they may provide for access into premises with the help of controller resetting.
- ❑ Do not lose Administrator and Engineer codes, otherwise you should reset controller to factory settings and reprogram it entirely.
- ❑ For all circuits connections, with the exception of power supply and electric lock control, 0.22 mm² cross area conductor shall be used. For power supply circuit and lock control it is desirable to use a conductor with 0.5 mm² cross area minimum.
- ❑ Do not connect a common wire of lock control circuit on the controller side, connect it on the side of the power supply.
- ❑ Bridge the electric lock with a varistor, or with a reverse included diode. This shall reduce the noise from electric lock windings interfering with controller standard performance.

Design

The controller has a 150 x 46 x 22 mm plastic case with a 2 x 6 (12 keys) film membrane keypad. Keypad design provides for 1,000,000 strokes minimum per each key.

On the back side of the controller there is an 8-wire cable for controller connection to hardware of access control system.

Controller is shown on current manual cover.

Controller Installation

Controller location should be chosen with regard to mounting and application convenience. Most common controller location is the wall at a lock handle level on the side opposite to door hinges. Figure 1 provides for controller installation diagram.

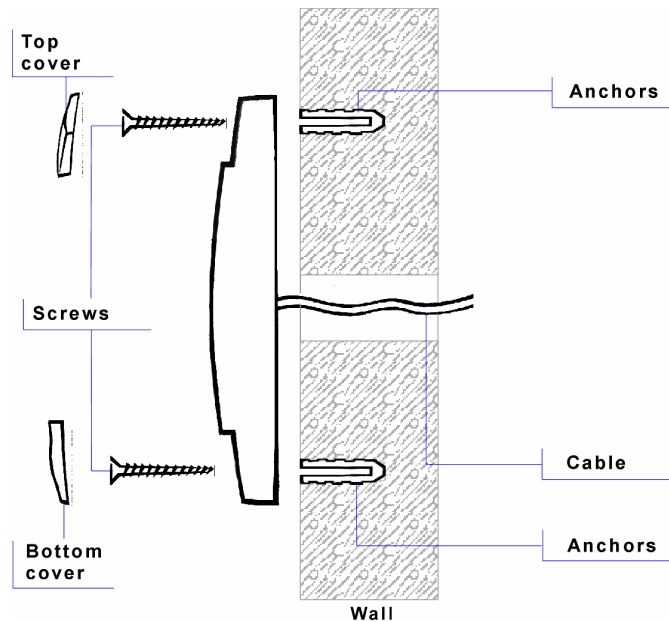


Figure 1. Controller installation

SC-06 controller installation procedures:

1. If top and bottom decorative covers of the controller are available, remove them with the help of a thin screwdriver or another flat tool. The bottom cover is marked with a logotype and the top one has a lens with a LED.
2. Drill two holes in the wall for enclosed anchors at a distance of 132 mm between hole centers.
3. Drill a hole for a cable in the wall under the central part of a controller case.
4. Connect controller to hardware (power supply, door contact, lock, RTE button). Next Subsection contains detailed information on controller connections.
5. Fasten controller case with two screws.
6. Latch the top and bottom covers. If necessary, the covers may be additionally fixed with a drop of nitric glue, on the other hand this will make controller disassembling problematic.

Controller Connection

External hardware shall be connected to the controller with the help of an 8-wire cable. Conductors are specified below in Table 1.

??????? 1

Conductor color	Output	Function
Red	+12	Controller power supply: +12...14 V, DC.
Black	GND	Common wire of power supply, door contact and RTE button.
White	DC	Normally closed door contact connection
Green	RTE/ER	Normally opened RTE button or external reader connection.
Brown	L+	Lock control, key output.
Blue	L-	Lock control common wire.
Orange	ALARM	Alarm Output.
Yellow	HLD/SNS	Hardware hold input or external alarm sensor input.

RTE/ER ? HLD/SNS inputs are multifunctional and their function is specified by Engineer during controller programming.

Factory Configuration

Connection layout shall vary subject to controller configuration. Figure 2 provides for controller connection layout under factory configuration (refer to Section «Controller Factory Settings».) Application of factory configuration does not require for programming with the exception of entering of Engineer, Administrator and users codes.

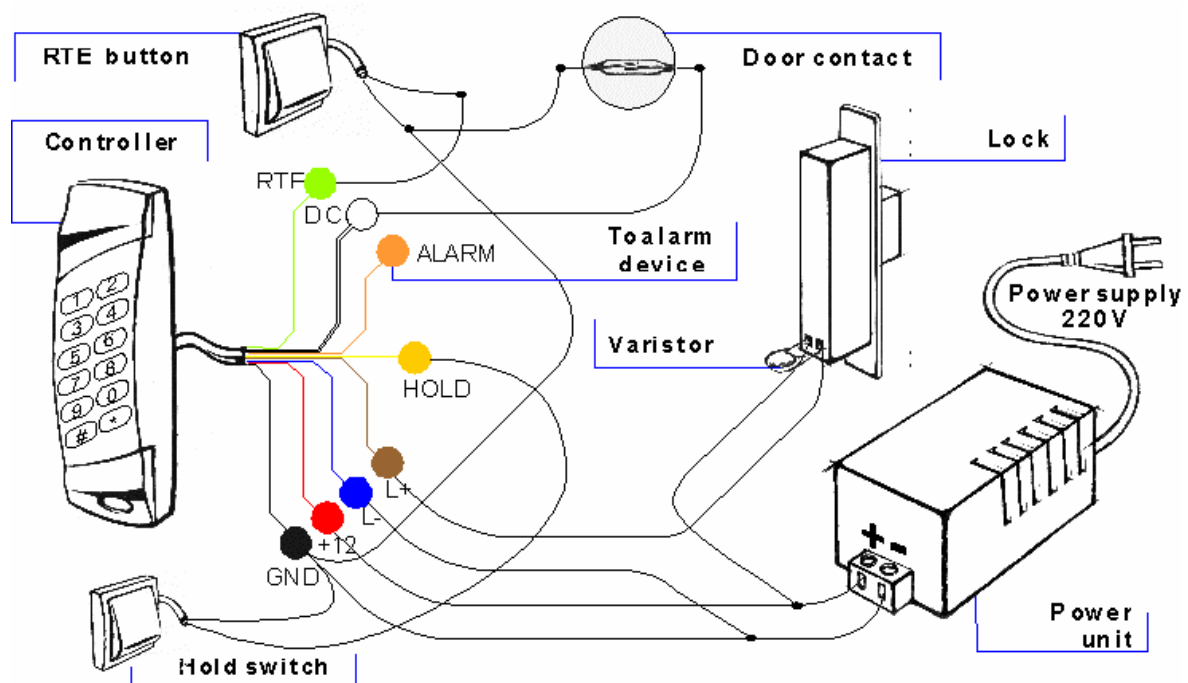


Figure 2. Connection of factory configured controller.

Factory configured controller supports the following hardware:

- ❑ Voltage-opened electric lock or strike. To be connected in accordance with circuit diagram (Figure 2).
- ❑ Request to Exit Button. Normally opened it should be connected between RTE/ER and GND outputs (green and black wires, respectively).
- ❑ Door Contact. Normally closed it should be connected between DC and GND outputs (white and black wires, respectively). If DC is not installed, DC and GND outputs shall be closed (interconnected).
- ❑ Hold switch. Normally opened it should be connected between HLD/SNS and GND outputs (yellow and black wires, respectively).
- ❑ Alarm Device. To be connected in accordance with circuit diagram (Figure 2).

Alarm Sensor Mode

Additional alarm sensor shall be connected in accordance with circuit diagram as per Figure 3. If necessary, the sensor and controller shall be powered from one power supply. If sensor is powered from an individual power supply, it is necessary to unite GND wires (common wires) of both power supplies. The rest elements of the system shall be connected in accordance with the above instructions (Figure 2).

Operation mode with extra alarm sensor shall be enabled with the help of Engineer command (refer to Controller Programming Section).

If alarm sensor is installed, hold mode cannot be enabled (with the help of a switch) as the alarm sensor is connected to a cable yellow wire instead of the switch.

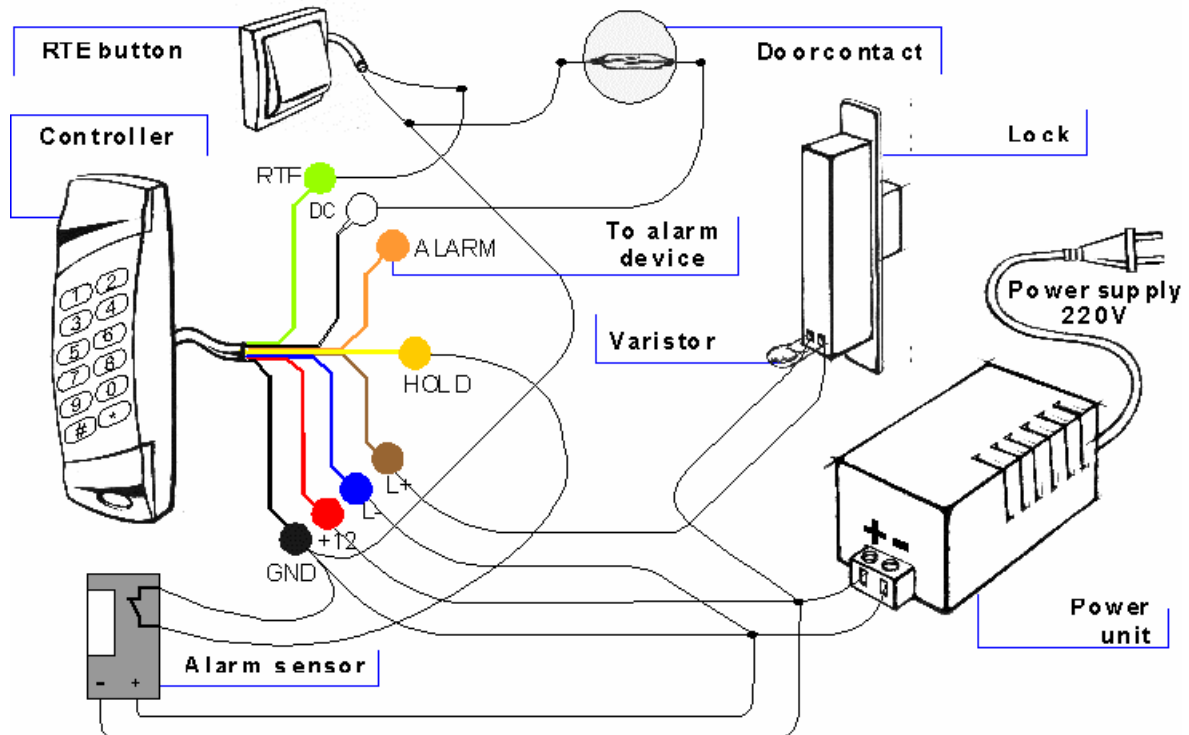


Figure 3. Alarm sensor Connection

Additional Reader Mode

Sometimes it is necessary to install an outside vandal-proof reader, or to provide both entry and exit to/from premises with the help of key. In this case the outside reader shall be installed (it is connected instead of request to exit button) and the controller shall be installed inside the premises. Figure 4 provides for controller connection circuit diagram. Controller compatible readers are listed in Complete Delivery and Warranties Section.

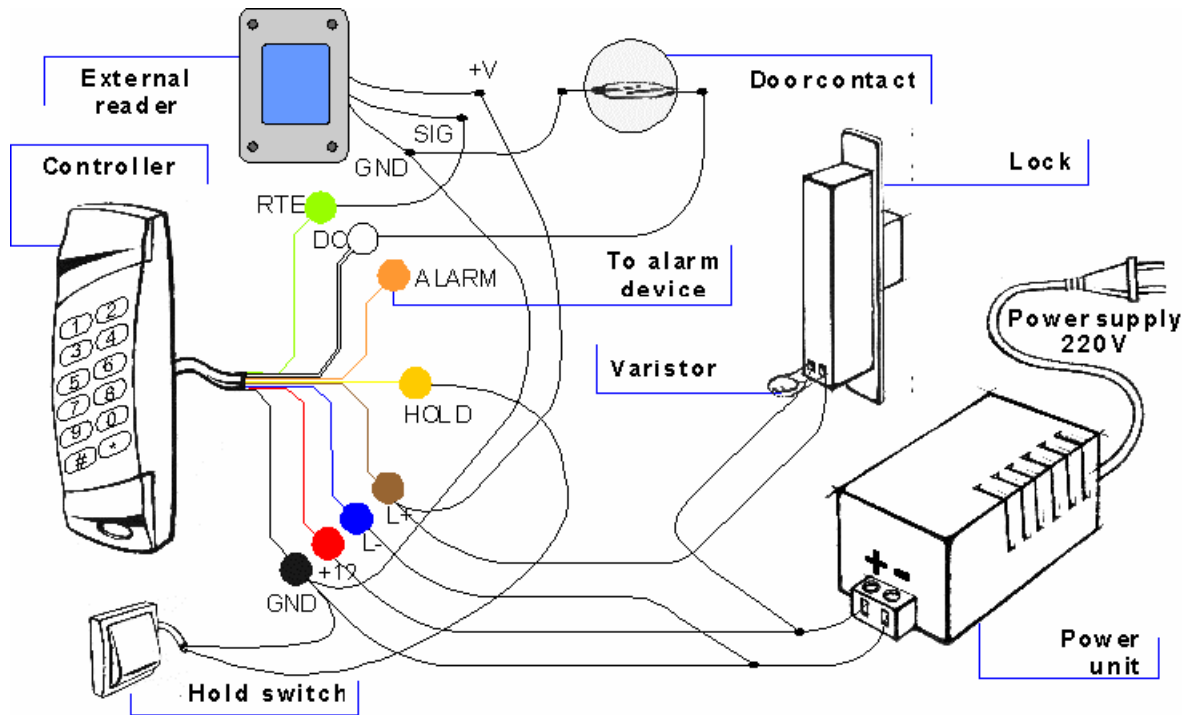


Figure 4. External reader connection

Operation mode with external reader shall be enabled with the help of Engineer command (refer to Controller Programming Section).

Lock And Alarm Device Digital Control

When it is necessary to insure reliable protection of the premises with external reader, digital control of the lock and alarm device may be used. In this case the door would not open even if the intruder tears the controller off the wall and powers lock control cable, because a special code formed by the controller is necessary to unlock the door.

At such configuration the lock and alarm device shall be connected via a special decoder located in a safe place. The above is explained in Figure 5.

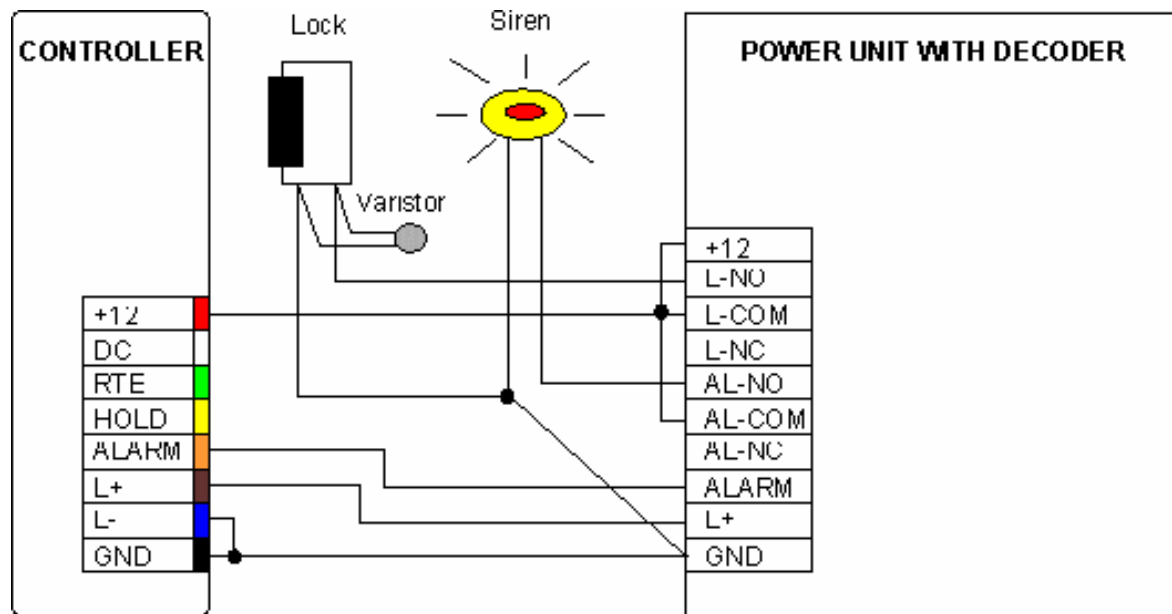


Figure 5. Lock and siren control via decoder



Caution! Even if it is necessary to control the lock only (alarm device control is not necessary), both controller outputs (brown and orange wires) shall be connected to decoder.

When operation mode with decoder is used, lock and alarm device digital control shall be enabled with the help of Engineer command (refer to Controller Programming Section).

Make sure that you have selected the right lock outputs to be connected to power supply, as well as the lock is bridged with varistor.

7. Controller programming

General Information

Controller configuration and settings, such as lock time, availability of extra alarm sensor, etc., can be changed with the help of Engineer code.

Administrator code provides for adding, removing and changing of users' access rights and PIN-codes.

The user with appropriate privileges can enter a number of commands. These are commands enabling security mode, enabling/disabling hold mode.



Programming mode can be enabled from a stand-by mode only. When hold or security mode is enabled, controller resetting or users' database changing is impossible.

Indication During Programming

Programming procedures are accompanied with sound and light indication.

Each key pressing is followed with a short sound (beep).

It is necessary to press "#" button after keying of each element (Engineer code, function code, value). On analysis of the entered value the correct command is verified with a long beep. In case of incorrect command the controller produces 3 short beeps.

On presentation of Master card substituting Engineer or Administrator code "#" button has not to be pressed.

Three short beeps are indicative of the error. Other indication options are presented in appropriate Sections. Watch LED indicator for verification of right procedures.

Symbols

The following symbols are used during programming procedures:

Symbol	Symbol description
	A proper color LED is continuously on.
	A proper color LED is blinking.

Keystroke is marked with a square having a key indication, for example, Key "5" stroke will look like this:

5

and entering of an arbitrary combination of three figures plus "#" will look like as follows:

X X X #

Beeps are marked as follows:

Symbol	Symbol description
	Short beep.
	Long beep.

If a card (key) has to be presented during programming, it is shown with the help of the following symbols:

Symbol	Symbol description
	Engineer card presentation.
	Administrator card presentation.
	User card presentation.

Beeps accompanying keystrokes are not displayed for command mnemonics obviousness.

Initial Authorization

New controller has no Engineer and Administrator codes in its memory, so prior to a new controller programming it is necessary to enter Engineer code.

Then Administrator code should be entered to ensure the capability to work with users' database (adding, removing and changing users' rights).

Initially Administrator code shall be entered by Engineer. When Administrator code has once been entered it can be changed only with the help of Administrator code. This procedure was arranged to separate functions of system configuring and personnel rights control between a system fixer (who may be the employee of another company) and a person responsible for access rights control: as a rule it is the company employee operating a controller.

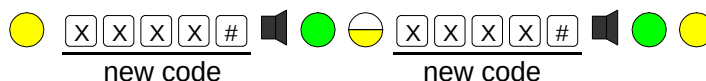
Engineer Code Creation

At first activation, when Engineer code is not available in controller, a yellow LED is on and controller produces long beeps at 3 seconds intervals. Controller preserves this state until Engineer code is entered. Controller also switches to this state after forced reset of its factory settings.



Incorrect entry of Engineer and Administrator codes will result in failure of access to the controller and the latter has to be reset to factory settings. That is why Engineer and Administrator codes shall be repeatedly entered to avoid error.

Engineer code initial entry shall be performed as follows:



Engineer code may include from 4 to 8 figures. If code entry is not correct the controller produces 3 short beeps and returns to the beginning of the procedures.

If Engineer code entry is correct the controller switches to Engineer mode that suggests immediate entry of Administrator code.

If Administrator code entry is supposed to be delayed, press 0 key three times and then press # key or wait 15 seconds to switch to a stand-by mode. Stand-by mode is indicated with a red LED.



9999 is a reserved combination and it cannot be used as Engineer code.

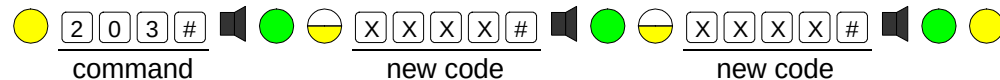
Administrator Code Creation

Administrator code may be entered immediately after Engineer code entry (refer to the above Subsection) or after switching to a stand-by mode.



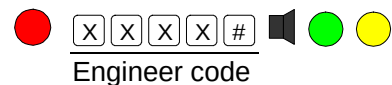
Initially Administrator code is entered with the help of Engineer code. Then Engineer code is not valid for this procedure, the Administrator code is required for access to Administrator code change;

Initial Administrator code entry from Engineer mode is as follows:

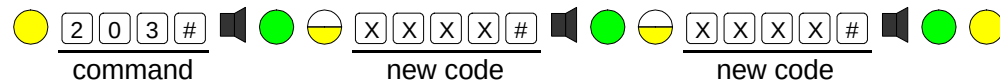


In a stand-by mode Administrator code shall be entered as follows:

enter Engineer code and press “#” key:



now enter the above described succession:



Then the controller keeps to Engineer mode which it exits automatically 15 seconds later or on entry of the following combination:





The above combination is a universal way of switching to a stand-by mode from at stage of programming procedure.



**Administrator code shall not coincide with Engineer code.
Controller shall not permit to enter coinciding codes.**

Access Code Change

Sometimes it is necessary to change Engineer and Administrator codes. Appropriate procedures are described below.

Besides, Engineer and Administrator codes can be supplemented with the card (key) to simplify entry to programming mode. If Engineer code is available, it is not necessary to enter the code and “#” sign to switch to programming mode: just present a card to controller reader to replace these steps.

Engineer Code Change

To change Engineer code it is necessary to know the old Engineer code. Code change procedure is as follows. Switch first to Engineer mode:

     
old Engineer code

or present Engineer card (if it has been previously entered into controller memory) and then enter the command of Engineer code change:

              
command new code new code

Engineer Card Adding/Change

To add or change Engineer card (key) follow the similar procedures. Both Engineer code, and Engineer card (if Engineer card has already been entered) may be used to switch to the mode. Controller stores only one Engineer card.

Engineer card adding/changing procedure with the help of code is as follows:

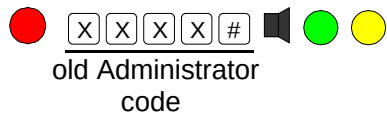
           
Engineer code command card

Or with the help of the previously entered Engineer card:

           
old card command new card

Administrator Code Change

To change Administrator code it is necessary to know the old Administrator code. Code change procedure is as follows. Switch first to Administrator mode:



or present Administrator card (if it has been previously entered into controller memory) and then enter the command of Administrator code change:



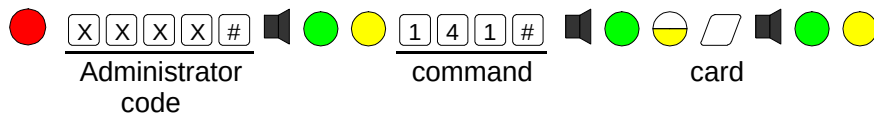
Administrator Card Adding/Change

To add or change Administrator card (key) follow the similar procedures. Both Administrator code, and Administrator card (if Administrator card has already been entered) may be used to switch to the mode. Controller stores only one Administrator card.

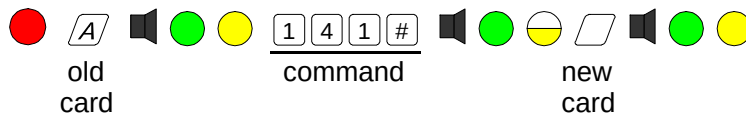


Engineer and Administrator cards shall be different: controller shall not permit to enter the same card twice with different functions. This is also the reason why user cards cannot be used as Engineer or Administrator cards.

To add/change Engineer card with the help of code proceed as follows:



or with the help of the previously entered Administrator card:



Controller Configuration (Engineer Commands)

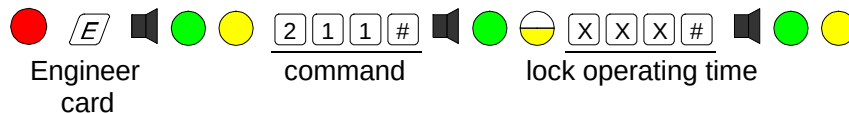
Controller is configured with the help of Engineer code or card and provides for setup of connected hardware and timing data.

Lock Operating Time Setup

Lock operating time can be preset within a range from 0 to 255 seconds with 0 corresponding to 256 seconds. The following steps are required to setup lock operating time:



or with the help of Engineer Card:



When small values are entered leading zeroes are not required. Controller shall not permit to enter values exceeding 255 seconds. Default value (factory setting) is 3 seconds.

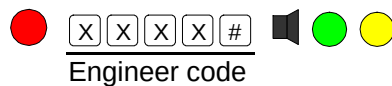
Lock Type Setup

Controller can support several types of locks: voltage-opened and voltage-closed. Besides, the controller can be configured to operate a lock with mechanical relock.



The controller default settings provide for control of a voltage-opened lock without mechanical relock.

Lock type setup is exercised with Engineer commands. Engineer mode is enabled with the help of Engineer code and “#” sign entry from a keypad:



or by presentation of Engineer card (if it has been preliminary entered):



Engineer mode enabling is indicated with a yellow LED light. You can consequently exercise commands required for programming of controller settings. Key the following command to switch back to a stand-by mode:



or wait 15 seconds and the controller shall switch to a stand-by mode automatically.

Table below provides for commands necessary for lock type setup. Remember that commands shall be entered in Engineer mode.

Lock type	Command
Voltage-opened lock	 <u>2</u> <u>2</u> <u>3</u> <u>#</u>    <u>1</u> <u>#</u>   
Voltage-closed lock	 <u>2</u> <u>2</u> <u>3</u> <u>#</u>    <u>0</u> <u>#</u>   
Lock with mechanical reload	 <u>2</u> <u>2</u> <u>4</u> <u>#</u>    <u>0</u> <u>#</u>   
Lock with mechanical reload	 <u>2</u> <u>2</u> <u>4</u> <u>#</u>    <u>1</u> <u>#</u>   

Lock Trigger Mode

Lock control output can be connected for performance in trigger mode when each presentation of a user card (or PIN-code keying) switches the lock to the opposite state. Such a mode can be used to control, for example, a security panel. Trigger mode is default disabled. Table below shows the commands for trigger mode enabling/disabling.

Trigger mode	Command
Enable	 <u>2</u> <u>2</u> <u>5</u> <u>#</u>    <u>0</u> <u>#</u>   
Disable	 <u>2</u> <u>2</u> <u>5</u> <u>#</u>    <u>1</u> <u>#</u>   

Lock Digital Control

Controller supports two lock control modes: common and digital. In common mode (factory settings) the lock is connected directly to controller outputs.



When digital control is used the lock is connected via a special decoder circuit board, which may be located in a power supply case, for example.

Figure 5 provides for lock connection diagram via decoder circuit board. Lock control mode is switched with the help of the following Engineer commands:

Lock Digital Control	Command
Enable	 <u>2</u> <u>2</u> <u>6</u> <u>#</u>    <u>0</u> <u>#</u>   
Disable	 <u>2</u> <u>2</u> <u>6</u> <u>#</u>    <u>1</u> <u>#</u>   

Lock digital control improves system tamper response security, because even if the controller is removed from the wall to get access to a lock control cable, it is impossible to open it.



Caution! Simultaneously with switching of lock control mode the alarm output operation mode gets switched as well. When lock digital control is applied the alarm device shall be necessarily connected to decoder circuit board output.

RTE/ER Input Function Programming

Normally opened request to exit button (RTE) for door opening from the inside, or the additional reader can be connected to RTE input. In latter case the controller can be located on the inner side of the door in a more secure place, and a vandal-proof reader can be installed outside. Controller connection diagrams are shown in Figures 2 and 4.

The following commands are used for programming of input function in Engineer mode:

RTE/ER Input Function	Command
RTE button	 <u>2</u> <u>2</u> <u>1</u> <u>#</u>    <u>1</u> <u>#</u>   
External reader	 <u>2</u> <u>2</u> <u>1</u> <u>#</u>    <u>0</u> <u>#</u>   



External reader functions are as follows: to open the door, to enable/disable security system. It is impossible to program the controller from external reader.

HLD/SNS Input Programming

HLD/SNS input can be used either for connection of a normally opened hold switch (Figure 2), or for connection of additional alarm sensor (Figure 3).

The following commands are used in Engineer mode for HLD/SNS input function switching:

HLD/SNS Input Function	Command
Hold switch input	 <u>2</u> <u>2</u> <u>2</u> <u>#</u>    <u>1</u> <u>#</u>   
Alarm sensor input	 <u>2</u> <u>2</u> <u>2</u> <u>#</u>    <u>0</u> <u>#</u>   

Access Code Tampering Security

The controller has a function of access code or card tampering security. It works as follows. In case 8 different incorrect PIN-codes entered or 8 different cards presented which are not recorded in controller database, the controller disables the reading function for 1 minute.

This slows down the process of access code or card tampering ten-folds and makes tampering almost impossible.



In addition a code tampering alarm may also be connected as described below.

Access code tampering security mode is enabled and disabled with the following commands in Engineer mode:

Access code tampering security	Command
Enable	 <u>2</u> <u>2</u> <u>7</u> <u>#</u>    <u>1</u> <u>#</u>   
Disable	 <u>2</u> <u>2</u> <u>7</u> <u>#</u>    <u>0</u> <u>#</u>   

Alarm Output Configuration

Alarm output can perform as normally opened or normally closed contact. In the first case when alarm is initiated the output gets closed to common wire. In the second case at normal state the output is closed to common wire and when alarm is initiated it gets opened.

Alarm can be initiated in various situations. Thus, when alarm sensor is activated at enabled security mode the alarm is always initiated. At other events the alarm can be either initiated or not.

Below there are commands for alarm output configuration in Engineer mode:

Alarm output	Command
Normally opened	 <u>2</u> <u>3</u> <u>1</u> <u>#</u>    <u>1</u> <u>#</u>   
Normally closed	 <u>2</u> <u>3</u> <u>1</u> <u>#</u>    <u>0</u> <u>#</u>   
Do not initiate tamper alarm when not in security mode	 <u>2</u> <u>3</u> <u>2</u> <u>#</u>    <u>1</u> <u>#</u>   
Initiate tamper alarm when in security mode	 <u>2</u> <u>3</u> <u>2</u> <u>#</u>    <u>0</u> <u>#</u>   
Disable open door alarm	 <u>2</u> <u>3</u> <u>3</u> <u>#</u>    <u>1</u> <u>#</u>   
Enable open door alarm	 <u>2</u> <u>3</u> <u>3</u> <u>#</u>    <u>0</u> <u>#</u>   
Do not initiate access code tampering alarm	 <u>2</u> <u>3</u> <u>4</u> <u>#</u>    <u>1</u> <u>#</u>   
Initiate access code tampering alarm	 <u>2</u> <u>3</u> <u>4</u> <u>#</u>    <u>0</u> <u>#</u>   

Open Door Time Setup

Open Door Time is the period of time starting after lock operating time expires. If after open door time expiry the door is still left open the controller starts beeping. There are two ways to disable beeping:

- ☐ Close the door.
- ☐ Present a valid key.



Door state control is possible only in case if a normally opened door contact is installed.

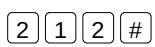
If open door time is set zero, door state control is disabled (default value is 30 seconds).

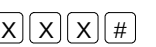
The controller can be programmed to enable alarm, if the door is left open during the period exceeding the preset time (refer to previous Subsection).



When small values are entered leading zeroes are not required. Controller shall not permit to enter values exceeding 255 seconds.

Open door time can be preset within a range from 0 to 255 seconds in Engineer mode (0 corresponds to 256 seconds) as follows:



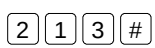
command door operating time

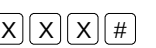
Exit Time Setup

If damping time is required for alarm sensor during security mode enabling, the appropriate exit time should be preset, which is a delay of actual enabling of controller security mode after proper procedure.

Factory preset exit time is 0; it means that security mode is enabled without any delay.

The following command is used to preset exit time in Engineer mode:

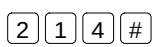


command exit time

Alarm Time Setup

Another controller parameter programmable by engineer, which can be preset within a range from 0 to 255 seconds, is alarm time. Note that 0 corresponds to alarm output activation on event e.g. until the source of alarm eliminates.

The following Engineer command is used to preset alarm time:



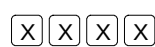



command alarm time

Administrator Commands

Administrator commands are purposed for user's database control: adding, removing, changing of rights, as well as changing of modes of access to premises. Besides, in Administrator mode it is possible to replace Administrator code for a new one as described above.

The controller is switched from a stand-by mode to Administrator mode with the help of Administrator code:



Administrator code

or with the help of Administrator card (if it has been preliminary entered):






One or several commands can be fulfilled after switching to Administrator mode. Enter the following command to switch back to a stand-by mode:

0 0 0 #   

or wait 15 seconds and the controller shall switch to a stand-by mode automatically.

Access Modes Control

Access to premises secured with **SC-06** Controller can be authorized by card only, by card plus code, and by card or code. Access modes can be switched with the help of the following commands:

Access mode	Command
Card only	 <u>1 3 2 #</u>   
Card plus code	 <u>1 3 1 #</u>   
Card or code	 <u>1 3 0 #</u>   

Users Editing

Administrator can add and remove individual users, as well as change their individual and group specifications. All users editing commands are described below.

User card adding

Users cards can be added one by one or several at a time (in a package) but into one group only. Adding procedure is as follows:

 1 2 1 #    X #        

command group number added cards

The Group No. specifies user privileges as follows:

Group number	User Category
1	Master
2	Privileged User
3	Guard
4	Common User

Enter the following command to finish up the procedure and to switch back to Administrator mode:

0 0 0 #   

or wait 15 seconds and the controller shall switch to a stand-by mode automatically.

While entering new cards the following sound indication is possible:



- the card has been successfully entered into database.



- database is full, no entry is possible.



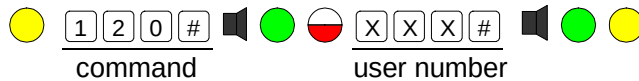
- the card is already available in database.



While entering new users they are consequently placed in the first vacant field of database. For example, if the users 1, 2, 3, 5, 6, 7 and 9 are available the next users shall be placed under number 4, then 8, and then 10, 11, etc.

User Deleting

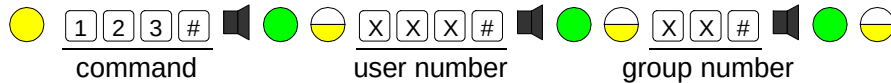
The user can be deleted from DB if user number is known. The following Administrator command is used to delete user:



If the card with the specified number is not available the controller produces 3 short beeps.

User Group Change

User rights are specified by the group the user belongs to: The following Administrator command is used to change user group:



or with the help of user card:



Yellow blinking LED indicates that the next user group can be edited by entering user number or presenting user card. Enter the following command to exit the mode:



Remember, that user rights are specified with regard to user group as follows:

Group number	User Category
1	Master
2	Privileged User
3	Guard
4	Common User

User Code Adding/Change

Each user has a default group PIN-code (PIN-code programming is described below.) If it is required to assign or change user individual code, apply the following Administrator command:

 1 2 2 #       X X X X #   

command card new PIN-code

Yellow blinking LED indicates that the next user PIN-code can be edited with the help of user card. Enter the following command to exit the mode:

0 0 0 #   

Remember, that PIN-code may include from 4 to 8 figures.



Individual user's codes must differ from other user's codes, Engineer, Administrator, group and duress codes.

Group Code Change

Each group has a group code that can be used when the user has no individual code; this provides for access code at all time.

Group PIN-code can be entered or changed with the help of the following Administrator commands:

Change group PIN-codes	Command (Group XXXX - PIN)
Group 1 (Master)	 <u>1 1 1 #</u>    <u>X X X X #</u>   
Group 1 (Privileged user)	 <u>1 1 2 #</u>    <u>X X X X #</u>   
Group 1 (Guard)	 <u>1 1 3 #</u>    <u>X X X X #</u>   
Group 1 (Common user)	 <u>1 1 4 #</u>    <u>X X X X #</u>   



Controller can perform in access mode with the help of group PIN-codes only, without cards, and for this purpose the codes have to be programmed with the help of the above command.

Database Clearing

All users and their individual PIN-codes can be cleared at once. The following Administrator command is used for this purpose:

 1 0 0 #    1 0 0 #   

As the procedure is irrevocable and will require for arrangement of a new users database the command has to be entered twice.



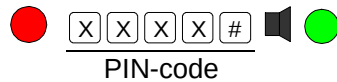
Group PIN-codes, Engineer and Administrator codes shall not be cleared under this procedure.

User Commands

Door Opening

All users available in database regardless of their belonging to any group have a right of access through a passageway controlled by the controller. Subject to the mode of access (card only, card or code, card plus code) the steps shall be as follows.

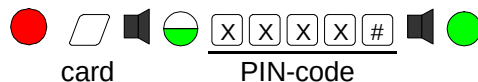
Access by code:



Access by card:



Access by card plus code:

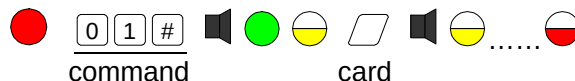


In Card plus code mode the user has to enter his PIN-code within 15 seconds maximum after card presentation. If the user has not entered his PIN-code within this period, the controller returns to a stand-by mode.

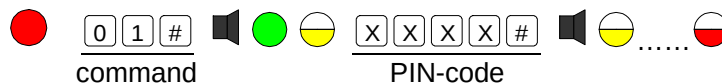
Privileged users can enable/disable security and hold controller modes.

Security Mode Enabling

Master and guard are permitted to use this command. Security mode is enabled with the help of the following command:



or with the help of code:



Yellow LED shall blink within time after card presentation or PIN-code entry. Blinking red LED is indicative of security mode enabled.

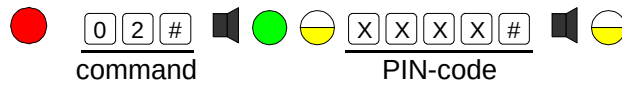


Only in case, when secure zones (either a door contact or an alarm sensor) are not active, the controller shall enable security mode after exit time expiry.

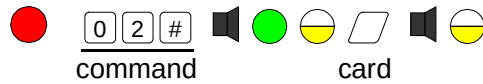
If security mode cannot be enabled due to alarm sensor or door contact activation, the controller produces 3 long beeps and returns to a stand-by mode. If the user has no right to enable security mode, the controller produces 3 short beeps and waits for acceptable PIN-code entry or presentation of a card with a required privilege.

Hold Mode Control

Hold mode can be enabled/disabled only by user having Master privileges. The following user command is used to enable a hold mode:

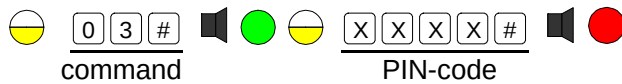


or with the help of card:

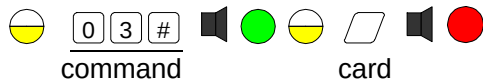


Yellow LED verifies acceptability of the command. Rarely blinking yellow LED after a long beep indicates hold mode. If the user has no proper privilege, the controller produces 3 short beeps and waits for acceptable PIN-code entry or presentation of a card with a proper privilege.

The following user command is used to disable a hold mode:



or with the help of card:



If the user has no right to disable hold mode, the controller produces 3 short beeps and waits for acceptable PIN-code entry or presentation of a card with a proper privilege. In case of no activities, after expiry of a 15 seconds period the controller returns to a hold mode (yellow LED blinks).

8. Return to Factory Settings

Return to factory settings can be required in various cases, if a second-hand controller without information on its settings is used or if programming procedures got confused and the way out cannot be found, etc.

The initial controller configuration is restored in case of returning to factory settings, as well as lock and door operating time, and exit time.

The procedures are as follows:

1. Power off the controller.
2. Press and hold “#” key.
3. Power the controller on. Note that red LED starts blinking.
4. 15 seconds later the controller produces a long beep followed by a flash of a green LED.
5. Release “#” key. Controller returns to factory settings and switches to a mode when Engineer code can be entered.



Engineer and Administrator codes and group PIN-codes are cleared and factory settings of connected hardware and timing data restores. User's database is left saved and unchanged.

9. Controller Performance

Subject to hardware configuration the controller can perform in various modes as described in Section 2.

Below several specific modes of controller performance are detailed.

Hold Mode

This mode can be enabled with the help of hardware (if HLD/SNS input is configured for performance with a hold switch: factory setting), or with a proper command entered with the help of a keypad by user having this privilege (only Master enjoys it).

Only Master and a privileged user have access through the door in hold mode. Guard and common user have no access to premises when hold mode is enabled.

Hold mode enabled with the help of hardware (with a hold mode switch) may be disabled with a command from a keypad. To enable a hold mode again a hold switch has to be switched off and on again.

Security Mode

Controller supports security mode functions. Depending on configuration the sensors are: either a door contact only (factory setting), or a door contact and external sensor connected to HLD/SNS input. For this purpose first configure HDL/SNS input for performance with alarm sensor with the help of a proper Engineer command.

Only Master and guard can enable/disable security mode. Note that the only thing you have to do to disable security mode is to present a card, to enter code or to present a card plus enter code (with regard to access mode). Security mode shall be disabled and the door opened.

If in security mode there is a tamper (either a door contact or an alarm sensor gets activated) the controller shall initiate alarm. If the alarm has specific time settings, it shall be disabled automatically after alarm time expiry. In case of alarm setting on event, it shall be disabled only after alarm cause (source) elimination.

Regardless of alarm mode (by time or on event) the alarm can be disabled by presentation of any card of proper privilege available in controller database.

Alarms

Controller can initiate alarms in various situations. Activation of a door contact or alarm sensor, as well as duress passage (refer below) always initiates alarm.

In other cases alarm can be enabled or not subject to settings introduced by Engineer. Alarms are programmed to be enabled in following cases:

- ☐ Tamper at disabled security mode, when the door is opened aside from controller.
- ☐ If the door is left open after open door time expiry.
- ☐ In case of access card or code tampering attempt.

Duress Mode

At access by PIN-code or by card plus PIN-code the controller supports a duress mode, or a duress access mode.

If you are forced to open the door with the help of your code it is necessary to enter a code that varies from your actual code by +1. In this case the controller opens the door and at the same time it activates alarm output providing a warning to a security service that you are forced to open the door.

For example, if your code is 12345 enter 12346. If your code is 12349 enter 12340 to initiate alarm.

As duress codes are automatically calculated by controller they are reserved and a duress PIN-code of one user cannot be assigned as a PIN-code to another user. The controller shall advise you that a certain code is already available in database.

10. Technical Specifications

Source voltage	12V, DC; regulated power supply is required
Consumption current	100 mA maximum
Lock maximum current	0.7 A for voltage-closed and 1.0 A for voltage-opened locks
Lock Operating Time	From 0 to 255 seconds
Door Operating Time	From 0 to 255 seconds. 0 value corresponds to no door state control
Exit time when security mode is enabled	From 0 to 255 seconds
Maximum users quantity	512 users, arbitrarily distributed into 4 categories

11. Complete Delivery and Warranties

Standard Delivery

Standard delivery includes as follows:

SC-06 Controller	1
Top cover	1
Bottom cover	1
Holdings and fasteners:	
Screws	2
Anchors	2
Certificate and brief User Manual	1
Complete Manual on a minidisk (MD-ROM)	1
Package box	1

Extra Hardware

External Readers

SC-03, **SC-04** and **SC-06** Stand-Alone Controllers operated in reader mode can be applied as external readers for two-way passageways. Table below contains instructions on appropriated controller transfer to reader mode.

Controller	Transfer to Reader Mode
SC-03 SC-04	Close Green (RTE) and Brown (L+) outputs
SC-06	If Engineer code has already been entered into the controller, reset it to factory settings. On controller initiation enter an Engineer code as follows:  <u>9 9 9 9 #</u>   Then the controller switches to external reader mode. To transfer it back to controller mode, reset it to factory settings.

Lock Digital Control Module

To provide for a lock digital control a special **LD-01** Decoder mounted on the side of an actuating device is applied.

Warranties

Manufacturer guaranties good product performance within one year from shipment date to Customer on condition of adherence to operation rules and parameters.