INT-R

UNIVERSAL EXPANDER FOR CARD / IBUTTON READERS

int-r_en 09/14

The INT-R expander interfaces with the INTEGRA, INTEGRA Plus and CA-64 alarm control panels, replacing the previously offered CA-64 SR and CA-64 DR expanders. This manual applies to the expander with electronics version 2.0 and firmware version 3.00 (or later).

1. Features

- Support for two proximity card / DALLAS iButton readers.
- Support for WIEGAND 26 interface readers.
- Arming / disarming and alarm clearing by using the readers.
- Access control features:
  - single door control,
  - relay output for control of electric strike, electromagnetic lock or another door actuator,
  - dedicated input for connecting a door opening sensor,
  - input for door unlocking with a button,
  - capability to automatically unlock the door in case of fire alarm.
- Control of 24. MONO SWITCH and 25. BI SWITCH type outputs.
- Additional NC type tamper input.
- Dedicated power supply connector socket.

The dedicated power supply unit can be connected to the expanders manufactured after 9 September 2014.

2. Specifications

Supply voltage	12 V DC ±15%
Standby current consumption	110 mA
Maximum current consumption	150 mA
Relay output rating (resistive load)	5 A / 30 V DC
+12V output rating	2.5 A / 12 V DC
Environmental class	II
Operating temperature range	-10 °C...+55 °C
Maximum humidity	93±3%
Dimensions	140 x 68 mm
Weight	80 g

The declaration of conformity may be consulted at www.satel.eu/ce

3. Electronics board

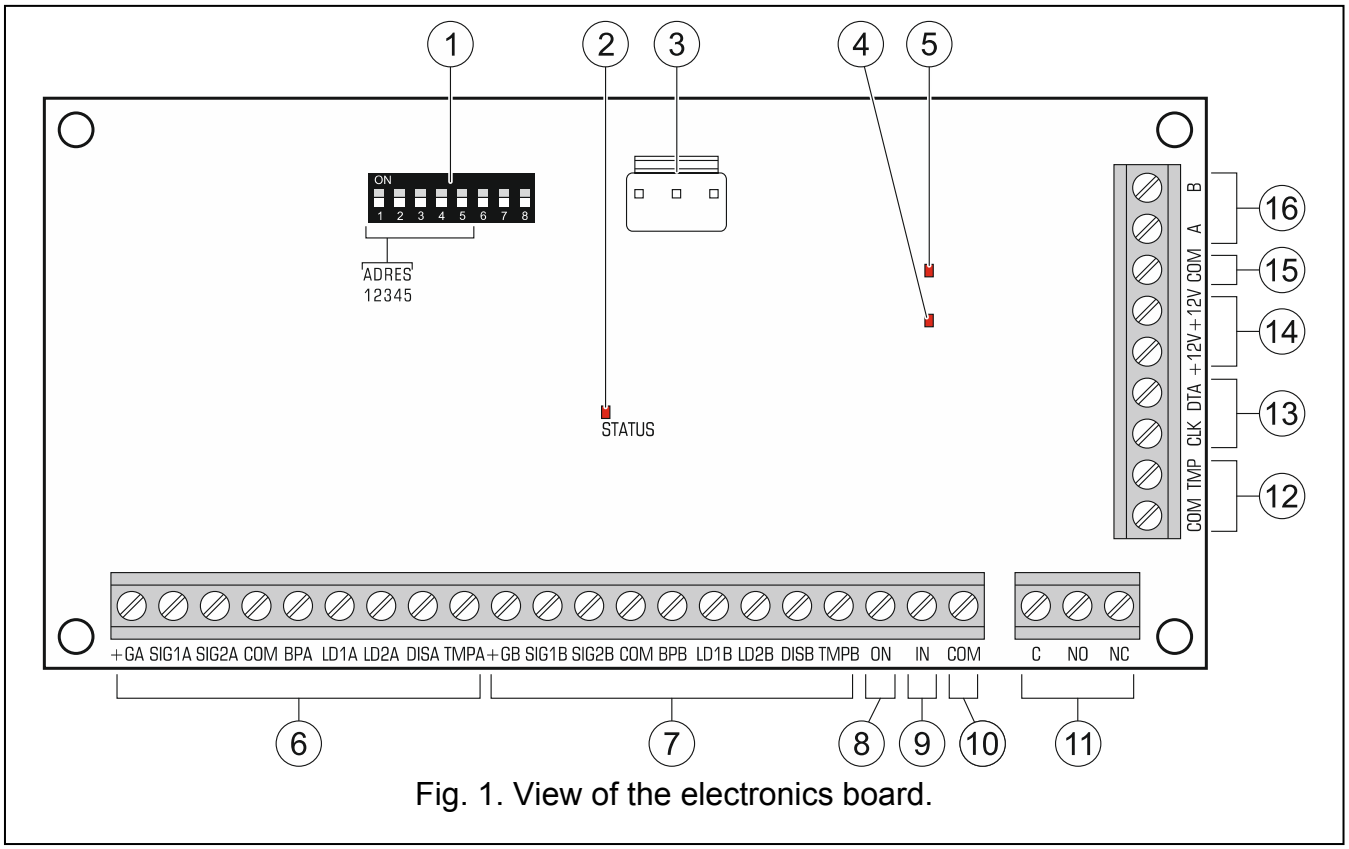

Fig. 1. View of the electronics board.

Explanations for Fig. 1:

(1) DIP-switches for setting address (see: „Address setting" p. 4).

(2) LED indicating the status of communication with the control panel:
ON – no communication with the control panel,
blinking – communication with the control panel OK.

(3) connector for a dedicated power supply unit (e.g. APS-412).

(4) LED indicator of the relay status (ON when the relay is active).

(5) LED indicator of power status (ON when power is present).

(6) terminals to connect the reader A (see: „Connecting the readers" p. 5).

(7) terminals to connect the reader B (see: „Connecting the readers" p. 5).

(8) NO type input for relay control (enables the door to be unlocked without using a reader).

(9) NC type input for door status control (if not used, it should be shorted to the common ground).

(10) common ground.

(11) relay terminals:
C - common contact,
NO - normally open contact,
NC - normally closed contact.

(12) tamper circuit terminals. The terminals should be short-circuited, if no tamper circuit is connected to them.

⑬ communication bus terminals.

⑭ +12 V DC inputs / outputs.

⑮ common ground.

⑯ RS-485 bus terminals.

4. Expander operating modes

The device can operate as:

I - CA-64 SR expander, supporting the CZ-EMM readers (CZ-EMM, CZ-EMM2, CZ-EMM3 and CZ-EMM4) manufactured from May 2005 **factory default setting**;

II - CA-64 SR expander, supporting the CZ-EMM readers manufactured until May 2005;

III - CA-64 SR expander, supporting the WIEGAND 26 interface readers;

IV - CA-64 DR expander, supporting the DALLAS iButton readers.

4.1 Changing expander operating mode

Disconnect power before performing steps 1 and 2.

1. Set the DIP-switches as required for the selected operating mode (see: Fig. 2).

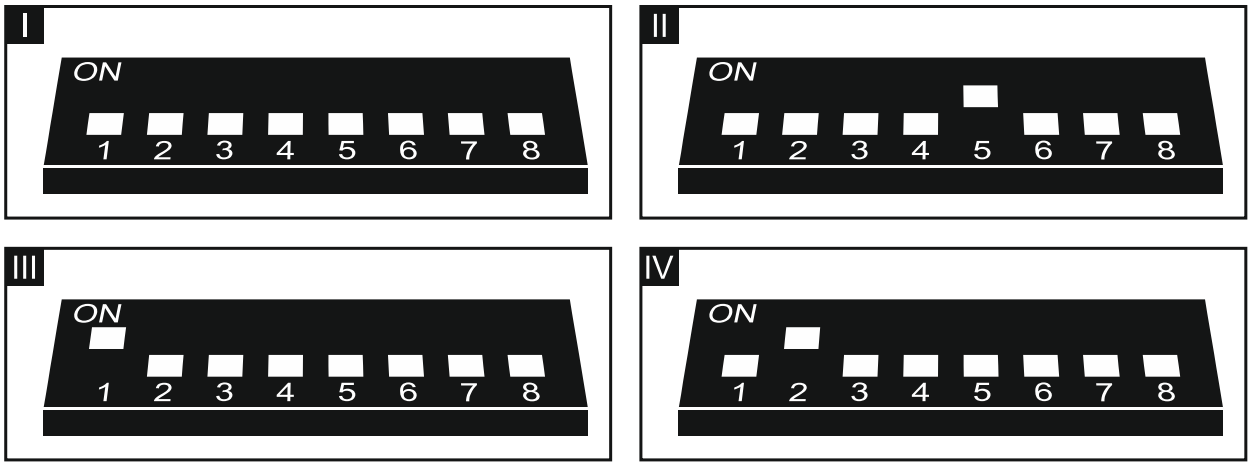

Fig. 2. The way of setting DIP-switches for the operating modes described above.

2. Short-circuit the CLK and DTA terminals.
3. Turn on the module power (connect the dedicated power supply unit to the connector on expander electronics board or connect the power wires to the +12V and COM terminals). The new operating mode will be saved, which will be indicated by slow blinking of the STATUS LED.
4. Turn off the module power.
5. Open the CLK and DTA terminals.

Note: *WIEGAND 26 interface readers, CZ-EMM series readers and keypads with readers can be used in the alarm system. Note, however, that the proximity card assigned to the user by means of a WIEGAND 26 interface reader will not be supported by readers which cannot work in this format. On the other hand, the WIEGAND 26 interface readers will not support cards assigned to the users by means of readers which cannot work in this format.*

5. Address setting

To set address, use the switches 1-5 of the DIP-switch package. A numerical value is assigned to each switch. In OFF position, the value is 0. Numerical values assigned to individual switches in ON position are shown in Table 1. The sum of numerical values assigned to switches 1-5 means the address set on the module. The address must be different from that on the other modules connected to the communication bus of the control panel.

DIP-switch number	1	2	3	4	5
Numerical value	**1**	**2**	**4**	**8**	**16**

Table 1.

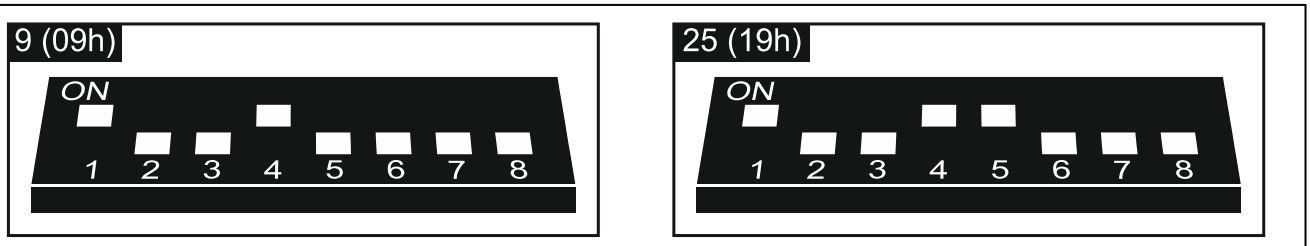

Fig. 3. Examples of address setting.

6. Installation and start-up

Disconnect power before making any electrical connections.

The expander is designed for indoor installation, in spaces with normal air humidity.

1. Fasten the expander electronics board in the enclosure.
2. Change the expander operating mode if it is to be different than the factory default one (see: „Expander operating modes” p. 3).
3. Set the expander address (see: „Address setting”).
4. Connect the CLK, DTA and COM terminals to the corresponding terminals of the control panel communication bus (see: installer manual for alarm control panel). It is recommended that an unshielded non-twisted cable be used to make the connection. If you use the twisted-pair type of cable, remember that CLK (clock) and DTA (data) signals must not be sent through one pair of twisted conductors. The conductors must be run in one cable. The cable length should not exceed 1000 m. If it exceeds 300 meters, it may be necessary to use several wires connected in parallel for each signal.
5. Connect readers to the respective terminals (see: „Connecting the readers” p. 5).
6. Connect the wires of door status sensor to the IN and COM terminals. If the door status is not to be monitored, connect the IN terminal to the expander COM terminal or, when configuring the expander, set value 0 for the MAX. DOOR OPEN TIME parameter.
7. Connect the electric strike, electromagnetic lock or another door actuator to the relay terminals.
8. If the door is to be unlocked by means of a monostable switch, connect the switch button to the ON and COM terminals.
9. If the expander is to supervise the enclosure tamper contact, connect the wires of tamper contact to the TMP and COM terminals. If the expander is not to supervise the enclosure tamper contact, connect the TMP terminal to the expander COM terminal.

10. Depending on the selected method of expander powering, connect the dedicated power supply unit to the connector on expander electronics board or connect the power wires to the +12V and COM terminals (the expander may be powered directly from the control panel, from an expander with power supply or from a power supply unit).

Do not connect power to the terminals, if the dedicated power supply unit is connected to the connector on electronics board.

11. Turn on the power.
12. Start the identification function in the control panel (see the control panel installer manual). Depending on the selected operating mode, the expander will be identified as CA-64 SR (expander for proximity card readers) or CA-64 DR (expander for DALLAS iButton readers).

6.1 Connecting the readers

The length of the cable connecting the reader and the expander should not exceed 30 m.

Connecting the proximity card readers

Connect the proximity card reader manufactured by SATEL to the expander terminals as displayed in Table 2.

Expander terminal		Terminal description	Color of reader wire
Reader A	Reader B		
+GA	**+GB**	+12 V DC power supply	red
SIG1A	**SIG1B**	data (0)	green
SIG2A	**SIG2B**	data (1)	black
COM	**COM**	common ground	blue
BPA	**BPB**	sound control (BEEPER)	yellow
LD1A	**LD1B**	green LED control	pink
LD2A	**LD2B**	red LED control	gray
DISA	**DISB**	disabling reader operation (HOLD)	brown
TMPA	**TMPB**	reader availability control	white

Table 2. The way of connecting wires of proximity card reader to terminals.

Notes:

- *In case of CZ-EMM3 and CZ-EMM4 readers the brown wire must be connected to the module.*
- *The black wire, which is available in the CZ-EMM3 and CZ-EMM4 readers, must be connected only when the expander and readers are to work in the WIEGAND 26 mode.*

Connecting the DALLAS iButton readers

Connect the DALLAS iButton reader to the expander terminals as displayed in Table 3.

Expander terminal		Terminal description	Color of reader wire
Reader A	Reader B		
SIG1A	**SIG1B**	data (0)	white
COM	**COM**	common ground	gray
			yellow
LD1A	**LD1B**	green LED control	green
LD2A	**LD2B**	red LED control	brown

Table 3. The way of connecting wires of DALLAS iButton reader to terminals.

7. Configuring

Parameters and options of the expander can be configured using:

- LCD keypad: ▶SERVICE MODE ▶STRUCTURE ▶HARDWARE ▶EXPANDERS ▶SETTINGS ▶*[module name]*;
- computer running DLOADX or DLOAD64 program: "Structure" window →"Hardware" tab →"Expansion modules" branch →*[module name]*.

7.1 Description of parameters and options

Given in square brackets are the names shown on the LCD keypad display.

Note: *Some parameters and options are not available in case of the expander operation with the CA-64 control panel.*

Name – individual name of the expander (up to 16 characters). In the LCD keypad, the name is programmed in the NAMES submenu (▶SERVICE MODE ▶STRUCTURE ▶HARDWARE ▶EXPANDERS ▶NAMES ▶*[module selection from list]*).

Partition – selection of the partition to which the expander is to belong (alarms from expander will be reported in this partition).

Lock [Lock feature] – if this option is enabled, module can perform access control functions. After activating the option, define how the relay is to operate:

ON if partition armed [On if part. armed] – relay is active when the partition is armed, and inactive when the partition is disarmed.

Note: *If the partition is disarmed in a different way than by means of the reader, the relay will only be deactivated after the reader reads out the code of proximity card / DALLAS iButton of an authorized user.*

Fixed ON time [ON time] – after reading the code of proximity card / DALLAS iButton, the relay is active for the RELAY ON TIME.

Fixed ON time – OFF if door open [ON, open->off] – after reading the code of proximity card / DALLAS iButton, the relay is active until the door is opened (the IN input is disconnected from the common ground), but not longer than for the RELAY ON TIME.

Fixed ON time – OFF if door closed [ON, close->off] – after reading the code of proximity card / DALLAS iButton, the relay is active until the door is closed (the IN input is reconnected to the common ground), but not longer than for the RELAY ON TIME.

Relay ON time – the time period during which the relay is active.

Max. door open time [Max. door open] – the maximum time period during which the door can remain open (the door status monitoring input can be disconnected from common ground). If the door is open for a longer time, appropriate information will be written into

the event log of the control panel (the proximity card readers will audibly signal the long opened door). If value 0 is programmed, the door status will not be monitored.

Dependent on door 1 [Dependent door1] / **Dependent on door 2** [Dependent door2] – you may define the door that must be closed to be able to unlock the door controlled by the partition keypad (to activate the relay). You can indicate a door supervised by another expander or an alarm system zone programmed as the 57. TECHNICAL – DOOR OPEN type.

No auto-disarm [Code* not dis.] – if this option is enabled, presenting the card to / touching the reader with DALLAS iButton will not disarm the system. In order to disarm the system, hold the card / iButton at the reader.

Access if armed [Code* in arm] – if this option is enabled, presenting the card to / touching the reader with DALLAS iButton will unlock the door controlled by the module even if the partition is armed. The option is available, if the NO AUTO-DISARM option is enabled.

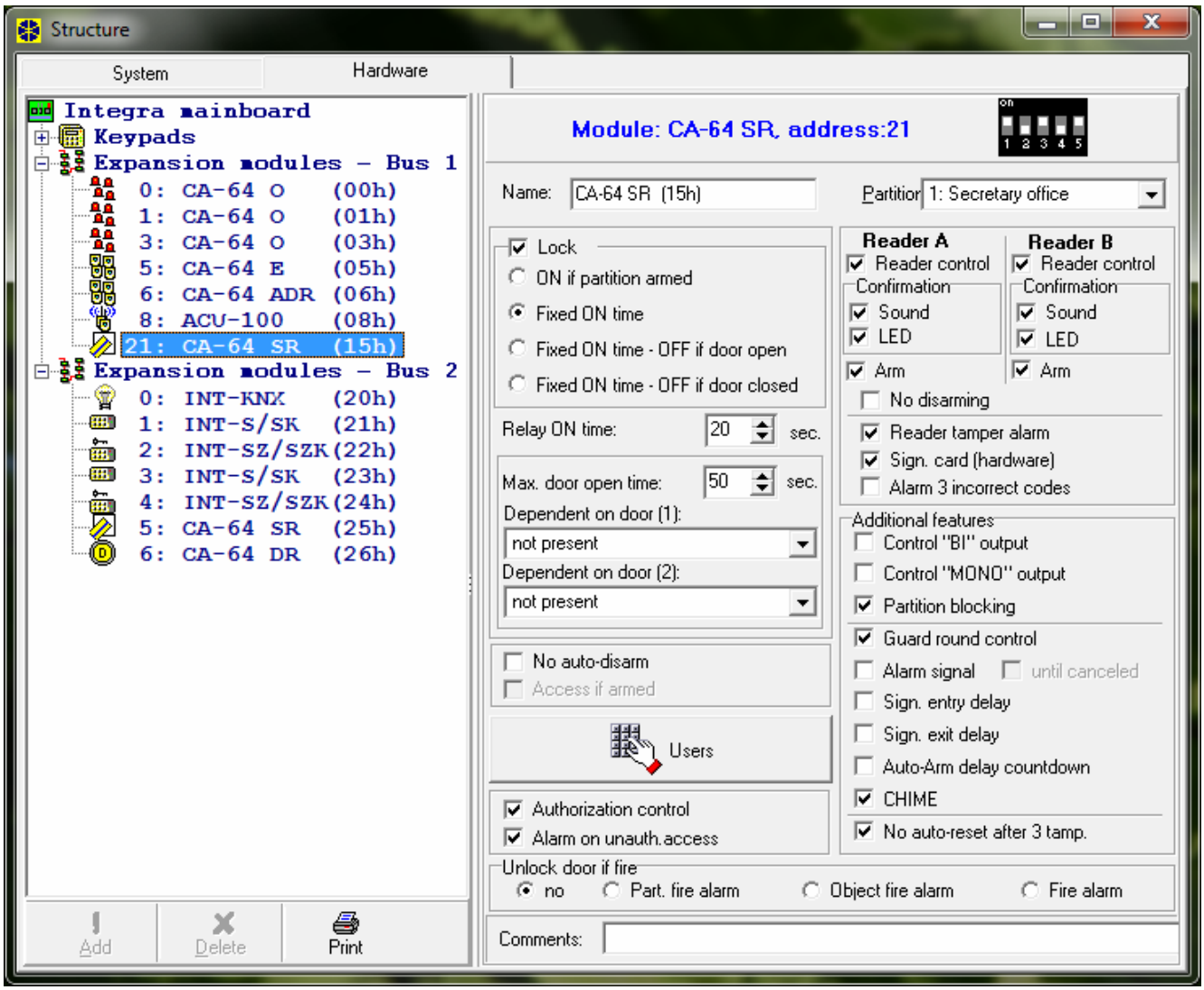

Fig. 3. Setting parameters and options for the expander identified as CA-64 SR in the DLOADX program.

Authorization control [Unauth. event] – if this option is enabled, unauthorized opening of the door will save the event to the control panel memory.

Alarm on unauth. access [Unauth. alarm] – if this option is enabled, unauthorized opening of the door when the partition is armed will trigger an alarm. The option is available if the AUTHORIZATION CONTROL option is enabled.

Users [Master users / Users] – indicate the administrators (master users) and users who will be authorized to use the readers connected to the expander.

Reader control (Reader A) [Reader A] / **Reader control (Reader B)** [Reader B] – options available in the expander identified as CA-64 SR. The expander can control the reader presence. Lack of the reader will generate a trouble (see also the READER TAMPER ALARM option). The reader presence control can be effected if the reader is provided with a presence control circuit (the white wire in proximity card readers manufactured by SATEL).

Confirmation: Sound (Reader A) [Reader A sound] / **Confirmation: Sound (Reader B)** [Reader B sound] – after reading the card code and its verification by the panel, the reader can inform the user by means of sounds whether the requested function will be executed or not (see: „Acoustic signaling" p. 10).

Confirmation: LED (Reader A) [Reader A LED] / **Confirmation: LED (Reader B)** [Reader B LED] – after reading the card / iButton code and its verification by the panel, the reader can inform the user by means of LEDs whether the requested function will be executed or not (see: „Optical signaling" p. 10).

Arm (Reader A) [Reader A arms] / **Arm (Reader B)** [Reader B arms] – if this option is enabled, the reader can be used for arming the partition to which the expander belongs.

No disarming [C.long not dis] – if this option is enabled, disarming by means of readers is impossible.

Reader tamper alarm [Al.rdrs tamper] – option available in the expander identified as CA-64 SR when the READER CONTROL option is enabled for reader A or B. If the option is enabled, lack of the reader will trigger tamper alarm.

Sign. card (hardware) [Hardw.signal.] – when this option is enabled, the reader will signal audibly the card code readout. This kind of signaling is useful, if there is a time lag between reading the card code and generating sound information after verification of the card code by the control panel.

Alarm 3 incorrect codes [3 wrong codes] – if the option is enabled, three times reading the code of an unknown card / iButton will trigger the alarm.

Control "BI" output [BI outs ctrl.] – using the card / iButton assigned to a code of the "BI" OUTPUT OPERATING type you can control the outputs of 25. BI SWITCH type.

Control "MONO" output [MONO outs ctr.] – using the card / iButton assigned to a code of the "MONO" OUTPUT OPERATING type you can activate the 24. MONO SWITCH type outputs.

Partition blocking [Part.blocking] – if this option is enabled, reading the card / iButton of the user who uses a code of the BLOCKING PARTITION or GUARD type will temporarily block the partition when armed (violating a zone belonging to the partition will not trigger any alarm). The time of blocking should be defined for the partition or the code (of the BLOCKING PARTITION type).

Guard round control [Guard control] – if this option is enabled, reading the card / iButton of the user who uses a code of the GUARD type will be recorded as completion of a guard round.

Alarm signal [Alarm (time)] – if this option is enabled, the proximity card readers will audibly signal alarms throughout the GLOBAL ALARM TIME.

until canceled [Alarm (latch)] – if this option is enabled, the proximity card readers will audibly signal alarms until they are cleared.

Sign. entry delay [Entry time] – if this option is enabled, the proximity card readers will audibly signal the entry delay countdown in the partition to which the expander belongs.

Sign. exit delay [Exit time] – if this option is enabled, the proximity card readers will audibly signal the exit delay countdown in the partition to which the expander belongs.

Auto-Arm delay countdown [Auto-arm delay] – if this option is enabled, the proximity card readers will audibly signal the auto-arming delay countdown in the partition to which the expander belongs.

CHIME [Chime zones] – if this option is enabled, the proximity card readers will audibly signal violation of zones with CHIME IN MODULE option enabled, belonging to the same partition as the module.

No auto-reset after 3 tamp. [No autorst.3t.] – if this option is enabled, the feature reducing the number of tamper alarms from the module to three is disabled (the feature prevents multiple logging of the same events and applies to successive uncleared alarms).

Unlock door if fire [Doors on fire] – you can define whether and when the fire alarm will unlock the door controlled by the expander (i.e. will activate the relay):

No [no open] – the door will not be unlocked in the event of fire alarm.

Part. fire alarm [on partit. fire] – the door will be unlocked in the event of fire alarm in the partition to which the expander belongs.

Object fire alarm [on object fire] – the door will be unlocked in the event of fire alarm in the object to which the expander belongs.

Fire alarm [on any fire] – the door will be unlocked in the event of fire alarm in the alarm system.

8. Using the readers

Description of adding proximity cards and DALLAS iButtons to the users can be found in the control panel user manual.

Functions that can be realized by the reader depend on the expander settings, alarm system status and user rights. It also depends on the expander settings whether the function will be performed after presenting the card to / touching the reader with the iButton, or after holding the card / iButton (the WIEGAND 26 interface readers do not support the card holding function). When read out, the card / iButton code is transmitted through the expander to the control panel. It is the control panel that decides whether and which function is to be performed. After receiving feedback from the panel, the reader can signal by means of LEDs or sounds whether the desired function will be executed or not.

Presenting the card to / touching the reader with the iButton will execute one or a few of the following functions:

- unlocking the door (activating the relay),
- disarming the partition to which the expander belongs,
- clearing alarm in the partition to which the expander belongs,
- toggling the status of 25. BI SWITCH type outputs,
- activating the 24. MONO SWITCH type outputs,
- confirming guard round,
- temporarily blocking the partition to which the expander belongs.

Holding the card / iButton at the reader will execute one or a few of the following functions:

- unlocking the door (activating the relay),
- starting the arming procedure / arming the partition to which the expander belongs,
- disarming the partition to which the expander belongs,
- clearing alarm in the partition to which the expander belongs,
- toggling the status of 25. BI SWITCH type outputs,
- activating the 24. MONO SWITCH type outputs,

- confirming guard round,
- temporarily blocking the partition to which the expander belongs.

Note: *When you activate the relay with the reader A, the "User access" event will be saved to the control panel memory. If the reader B is used to activate the relay, the "User exit" event will be saved.*

8.1 Optical signaling

The readers offered by SATEL come with one bicolor LED (emitting red and green light) or two LEDs (red and green).

Information on partition and expander status

The LEDs indicate status of the partition to which expander belongs, as well as lack of communication between the expander and the control panel.

Green LED lit – partition disarmed.

Green and red LED blinking alternately – alarm.

Red LED lit – partition armed.

Red LED blinking with increasing frequency – exit delay countdown.

Red LED blinking steadily – no communication between the expander and the control panel.

Signaling after readout of the card / iButton code

The signaling is provided by the LED which at the particular moment does not present information on the partition status, i.e. it can be either the green LED or the red one, depending on the circumstances.

2 short blinks repeated three times – the user of the given card / iButton should change the code.

3 short blinks – signaling of:

- starting the procedure of arming (there is exit delay in the partition) or arming (there is no exit delay in the partition),
- disarming and/or alarm clearing.

4 short blinks and 1 long blink – confirmation of function execution.

1 long blink – refusal to arm (there are violated zones in the partition or there is a trouble).

2 long blinks – unknown card / iButton.

3 long blinks – unavailable function.

8.2 Acoustic signaling

The proximity card readers offered by SATEL are equipped with a sounder. When using readers which have no sound signaling capability, you can connect an external piezoelectric transducer (5 V) to the expander for each reader (BPA and COM terminals for reader A, BPB and COM terminals for reader B).

Signaling events

Sounds can be used to transmit information on events in the partition to which the expander belongs, as well as on a long open door.

5 short beeps – zone violation (CHIME).

1 long beep every 3 seconds, followed by a series of short beeps for 10 seconds and 1 long beep – exit delay countdown (if the delay time is shorter than 10 seconds, only the final sequence of short beeps will be generated).

A sequence of 7 beeps of diminishing duration, repeated every few seconds – auto-arming delay countdown.

1 short beep every 150 ms – long open door.

2 short beeps every second – entry delay countdown.

Continuous beep – alarm.

1 long beep every second – fire alarm.

Note: *If the device is working as the CA-64 SR expander, which supports the CZ-EMM readers manufactured until May 2005, the alarm will be signaled in the same way as the fire alarm, i.e. by a long beep every second.*

Beeps generated when operating

1 short beep – confirmation of the card / iButton code readout.

2 short beeps repeated three times – the user of the given card / iButton should change the code.

3 short beeps – signaling of:

- starting the procedure of arming (there is exit delay in the partition) or arming (there is no exit delay in the partition),
- disarming and/or alarm clearing.

4 short beeps and 1 long beep – confirmation of function execution.

1 long beep – refusal to arm (there are violated zones in the partition or there is a trouble).

2 long beeps – unknown card / iButton.

3 long beeps – unavailable function.

SATEL sp. z o.o. • ul. Budowlanych 66 • 80-298 Gdańsk • POLAND
tel. + 48 58 320 94 00
info@satel.pl
www.satel.eu