

Alarm Control Panel

CA-64

Program Version 1.04.04

Satel 

GDAŃSK

INSTALLER MANUAL





WARNINGS

For safety reasons, the alarm system should only be installed by qualified personnel.

The control panel should be connected to **PSTN lines only**. Connecting the telephone circuit directly to digital network (e.g. ISDN) will cause damage to the equipment.

As the alarm system may contain hazardous items, its components should be kept out of reach of unauthorized personnel.

In order to avoid the risk of electric shock, read carefully this manual before proceeding to installation. Any connections should be made in deenergized state only (i.e. with power supply disconnected).

In the event of service operations consisting in fuse replacement, they must only be carried out after disconnecting the supply voltage. For the replacement, use only the fuses which have identical parameters as the original ones.



It is recommended that the manufacturer's prescribed housings and power supply units be used.

Making any construction changes or unauthorized repairs is prohibited. This applies, in particular, to modification of assemblies and components.

CAUTION !

It is impermissible to connect a fully discharged battery (with voltage on unloaded terminals less than 11V) to the alarm panel. To avoid hardware damage, the fully discharged or never used battery should be precharged with the use of a suitable charger.

The batteries used in the alarm systems contain lead. The used-up batteries must not be thrown away, but disposed of as required by the existing regulations (European Directives 91/157/EEC and 83/86/EEC).

DECLARATION OF CONFORMITY		
Product: CA64P – Control panel CA-64 main board	Manufacturer: SATEL spółka z o.o. ul. Schuberta 79 80-172 Gdańsk, POLAND tel. (+48 58) 320-94-00 fax. (+48 58) 320-94-01	
Product description: Main board for CA64 control panel intended for use in intruder alarm systems.		
This product meet the essential requirements and is in conformity with following EU Directives: LVD 73/23/EEC+93/68/EEC EMC 89/336/EWG + 91/263/EEC, 92/31EEC, 93/68/EEC R&TTE 1999/5/EC (network connection, TBR21)		
This product is compliant with the following harmonized standards: LVD: EN 50131-1:1997; EN 50131-6:1997; EN60950:2000, EN60335-1:1994/A1:1996 Annex B EMC: EN 55022:1998; EN 61000-3-2/-3; EN 50130-4:1995, EN 61000-4-2/-3/-4/-5/-6/-11 R&TTE: TBR 21(1998)		
Compliance with harmonized standards was checked in an accredited test house: „Electronic Technology Systems Dr. Genz GmbH”, Germany. LVD test report no: G0M20211-7290-L EMC test report no: G0M20211-7290-E-16 R&TTE test report no: G0M20211-7290-T-15 (TBR21)		
Gdańsk, Poland	06.05.2004	Head of Test Laboratory: Michał Konarski 
Latest EC declaration of conformity and product approval certificates can be downloaded from our Web site www.satel.pl		

CONTENTS

1. INTRODUCTION.....	3
2. GENERAL FEATURES OF CONTROL PANEL.....	3
3. SYSTEM COMPONENTS.....	4
3.1 MAINBOARD.....	4
3.2 LCD KEYPAD.....	5
3.3 SYNOPTIC BOARD.....	5
3.4 PARTITION KEYPAD.....	5
3.5 CODE LOCK.....	6
3.6 EXPANDER FOR THE PROXIMITY CARD READER OR DALLAS CHIP READER.....	6
3.7 ZONES EXPANDER.....	6
3.8 OUTPUTS EXPANDER.....	6
3.9 ZONES EXPANDER WITH POWER SUPPLY UNIT.....	6
3.10 OUTPUTS EXPANDER WITH POWER SUPPLY UNIT.....	6
3.11 ADDRESSABLE ZONES EXPANDER.....	6
3.12 VOICE SYNTHESIZER EXPANDER.....	7
4. FUNCTIONAL DESCRIPTION.....	7
4.1 OBJECTS.....	8
4.2 PARTITIONS.....	8
4.3 ZONES.....	12
4.3.1 Identification and numbering of zones in the system.....	12
4.3.2 Parameters.....	12
4.3.3 Options.....	13
4.3.4 Zone type.....	15
4.4 OUTPUTS.....	18
4.4.1 Parameters.....	18
4.4.2 Options.....	18
4.4.3 Source of output triggering.....	19
4.4.4 Clearance availability.....	19
4.4.5 Outputs type.....	19
4.5 CODES AND USERS.....	23
4.6 PREFIXES.....	25
4.7 MONITORING.....	25
4.8 MESSAGING.....	29
4.9 ANSWERING A PHONE CALL.....	31
4.9.1 Control via telephone.....	31
4.10 CONTROL OF OUTPUTS FROM LCD KEYPAD.....	31
4.11 REMOTE CONTROL.....	32
4.12 CONTROL PANEL STARTER.....	33
5. CONTROL PANEL INSTALLATION.....	33
5.1 CONNECTION OF POWER SUPPLY.....	36
5.1.1 Description of electric connections.....	36
5.1.2 Control panel power supply starting procedure:.....	36
5.2 CONNECTION OF LCD KEYPADS.....	37
5.3 CONNECTION OF EXPANSION MODULES.....	43
5.4 CONNECTION OF DETECTORS.....	45
5.5 CONNECTION OF SIGNALING DEVICES.....	47
5.6 CONNECTION OF TELEPHONE LINE.....	48
5.7 CONNECTION OF VOICE SYNTHESIZERS.....	48
5.8 CONNECTION OF PRINTER.....	49
5.9 CONNECTION OF SERVICE COMPUTER.....	49
5.10 CONNECTION OF EXTERNAL MODEM AND GSM-4 MODULE.....	50
6. STARTING THE CONTROL PANEL.....	53
6.1 STARTING THE SYSTEM.....	53

6.2	SERVICE MODE	53
6.2.1	<i>Service mode menu</i>	56
6.3	CONTROL PANEL PROGRAMMING	71
6.4	PROGRAMMING BY TELEPHONE	71
7.	BASIC TECHNICAL DATA	72
8.	HISTORY OF THE MANUAL UPDATES	74

1. INTRODUCTION

All parameters of the CA-64 alarm system can be **programmed** both with the use of a PC computer, as well as an LCD keypad (this information holds good to the software in version CA-64 v1.04.00 or later).

Detailed information about parameters of the alarm system software **is available in the „Help” system of the DLOAD64 program** purchased with the alarm control panel or, alternatively, at the web site *www.satel.pl*. In order to avail yourself of the system, install and run the program, and highlight the required element of the program window (to do so, move the mouse pointer to and click the left mouse key on the element) and then press the F1 key on the computer keyboard. Another way of getting access to the “Help” is by opening the “Information” drop-down menu and selecting the “Help” function.

2. GENERAL FEATURES OF CONTROL PANEL

The control panel CA-64 is designed for medium-size and larger sites. Owing to its expandability by adding modules, it is an ideal solution for facilities which are planned to be developed. It permits connecting a big number of keypads to control the system (theoretically 64+18, including those on computer screen), defining a big number of partitions, and it has a large number of supervision zones, thus enabling the security tasks to be reasonably solved in most facilities.

The control panel has many interesting features which give it a strong advantage in competition with other equipment of similar class.

- Processor system with software stored in the FLASH memory, which allows software updating and extension with new functions. New software version can be loaded via the control panel RS-232 port without removal of the panel from the site.
- Possibility to keep the parameters programmed by service personnel in the FLASH memory. Thus, even on disconnecting the memory back-up battery, the control panel restores settings made by the service.
- Possibility to divide the system into 8 objects and 32 partitions (partition = group of zones). The partitions may be controlled by the user, timers, control inputs, or their status may be dependent on the status of other partitions. It is possible to temporarily restrict the access to partitions.
- Possibility of system development by adding the extension modules to obtain up to 64 zones and outputs. Additionally, the modular system structure limits the number of cables.
- The system may store up to 192 codes which may be assigned either to users or control functions.
- Advanced functions of simultaneous system control by means of LCD keypads and user computers connected to them. Additionally, the service personnel may control the panel either via RS-232 port or via modem. It is possible to control individual partitions via partition keypads assigned to them.
- Possibility to control the access to selected parts of the facility by means of partition keypads, code locks, proximity card readers and DALLAS chips, which enable monitoring the access doors as well as controlling the locks (electric catches). The monitoring of door status does not reduce the number of zones controlled by the panel.
- Possibility to define the names of users and of majority of system components (partitions, zones, outputs, modules). This facilitates the control and monitoring of system as well as viewing of events log.

- Monitoring is carried out with the use of four different telephone numbers (two stations, each with a back-up number), with a possibility to divide events into 8 identifiers. Besides basic transmission formats, the control panel makes possible monitoring in Ademco Contact ID format.
- Reporting to 16 normal telephone numbers with the use of messages from voice synthesizers (up to 16 messages) or pagers (64 digital messages). Reception of message may be confirmed with a code sent by means of the telephone set keyboard (DTMF).
- Function of phone call answering, which enables checking the status of all control panel partitions and controlling of outputs (up to 16 outputs). This function is executed after user identification (each user may be assigned a special "phone call" code).
- Extended function of events printing, which enables event sorting. Event descriptions are in accordance with format Ademco Contact ID list of events, hence the printouts from the control panel correspond to those from the monitoring station. Besides, the names of zones, modules and users are printed as they are defined in the system.
- Additional function of control panel RS-232 port, i.e. controlling the external analog modem, ISDN modem, GSM-4 module or ISDN module of SATEL manufacture, enables communication to be established with the service computer. In this case, remote programming via telephone line and service are as quick as direct programming via RS-232 port.
- Possibility of time-based control owing to 64 timers that operate on week work cycle, with an option to define exception periods. Additionally, each partition is provided with its own timer (based on week cycle or day cycle), programmed by the suitably authorized user, to secure automatic arming and disarming.
- Facilitated performance of non-standard functions due to complex logic operations at outputs.
- High-capacity event log (6140 events) where, in addition to the monitored events also other events (like user access, functions used, etc.) are stored.

3. SYSTEM COMPONENTS

The control panel is provided with communication buses which permit connection of modules to improve hardware possibilities. Moreover, the software up-dating is possible, which makes upgrading of the system an easy task. It allows the system to be extended by new components which will be developed in future in order to meet customer's needs and requirements.

Described below are the already existing system components.

3.1 MAINBOARD

- 16 zones programmed individually to handle configurations NO, NC, EOL, 2EOL/NO and 2EOL/NC with functional test of the detector. One of a few dozens of response types can be chosen for each zone.
- 16 outputs with a programmable operating mode and a possibility to select one of a few dozens functions (including 4 high current outputs with electronic fuses and 12 low current outputs designed to control relays).
- 2 high current outputs with electronic fuses for "power supply output" function.
- 2 connectors for voice synthesizers SM-2 or CA-64 SM.
- Communication bus for connection of LCD keypads; 8 LCD keypads and synoptic board module may be connected to the bus.

- 2 buses for additional modules (expander buses), which enable 64 additional modules to be connected to the control panel. Zone modules, output modules, zone/output modules with power supply, partition keypads, code locks, proximity card readers and DALLAS chips and voice synthesizer expanders may be connected to the buses.
- Phone communicator, provided with a DTMF detection unit, enabling reception of commands via the telephone, monitoring, information and remote programming.
- RS-232 port enabling the alarm system operation by means of a computer (DLOAD64 installation program), operation with a printer and the use of an external modem.
- Switching-mode power supply of output load 3 A, with short circuit protection, provided with battery monitoring and discharged battery disconnection unit.
- Independent real time clock with calendar, provided with its own back-up battery.
- Visual signaling of operations of all outputs, battery charging circuit and telephone communication unit.
- Protection of all inputs, outputs and communication buses.

3.2 LCD KEYPAD

- Large, well-readable 2x16 characters display with permanent or temporary display backlighting activated on pressing a key or by any control panel zone.
- 16-key keyboard with backlighting controlled in the same way as the display backlighting.
- 2 zones with properties identical to main panel zones.
- Microswitch to detect keypad tampering.
- RS-232 port allowing the alarm system to be operated by means of computer (GUARD64 supervisory and user program – full monitoring of system status, virtual keypad, easier management of users).

3.3 SYNOPTIC BOARD

- Visualization of the state of all partitions and zones in the alarm system by means of LEDs.
- Two optional operating modes:
 - monitoring mode (with any number of boards connected)
 - keypad mode (with an option to define the way of LEDs blinking and a possibility to connect to the RS-323 port of a PC having the GUARD64 program installed).
- Switching-mode power supply with short-circuit protection.
- Battery charging and control system with disconnection of a discharged battery.
- Module tamper zone.

3.4 PARTITION KEYPAD

- 12-key keypad with permanent or temporary backlighting.
- 3 LEDs (ALARM, ARMED, TROUBLE) for showing the status of partition to which the keypad is assigned.
- Microswitch to detect keypad tampering.
- Relay for control of electric catch, lock or electromagnetic interlock.
- NO/NC zone for door status monitoring.

3.5 CODE LOCK

- 12-key keypad with permanent or temporary backlit.
- 3 LEDs, showing readiness, access allowed and, additionally, system trouble.
- Microswitch to detect code lock tampering.
- Relay for control of electric catch, lock or electromagnetic interlock.
- NO/NC input for door status monitoring.

3.6 EXPANDER FOR THE PROXIMITY CARD READER OR DALLAS CHIP READER

- One or two reading heads (recording entry and exit),
- Relay for electromagnetic door lock control,
- Input used to control the relay (NC),
- Input used for monitoring the door status (NC),
- Additional zone for monitoring the module tampering (NC).

3.7 ZONES EXPANDER

- 8 zones with properties identical to the main panel zones.
- Additional zone for monitoring the module tampering.

3.8 OUTPUTS EXPANDER

- 8 outputs with functional properties identical to the main panel outputs in three versions: 8 relay outputs, 8 outputs of OC type or 4 relay outputs/ 4 OC type outputs.
- Additional zone for monitoring the module tampering.

3.9 ZONES EXPANDER WITH POWER SUPPLY UNIT

- 8 zones with properties identical to the main panel zones.
- Additional zone for monitoring the module tampering.
- Switching-mode power supply, output load 2.2 A, with short circuit protection.
- Battery charging and control circuit with disconnecting the discharged battery.

3.10 OUTPUTS EXPANDER WITH POWER SUPPLY UNIT

- 8 outputs with functional properties identical to the mainboard outputs in three versions: 8 relay outputs, 8 outputs of OC type or 4 relay outputs/ 4 OC type outputs.
- Additional zone for monitoring the module tampering.
- Switching-mode power supply, output load 2.2 A, with short circuit protection.
- Battery charging and control circuit with disconnecting the discharged battery.

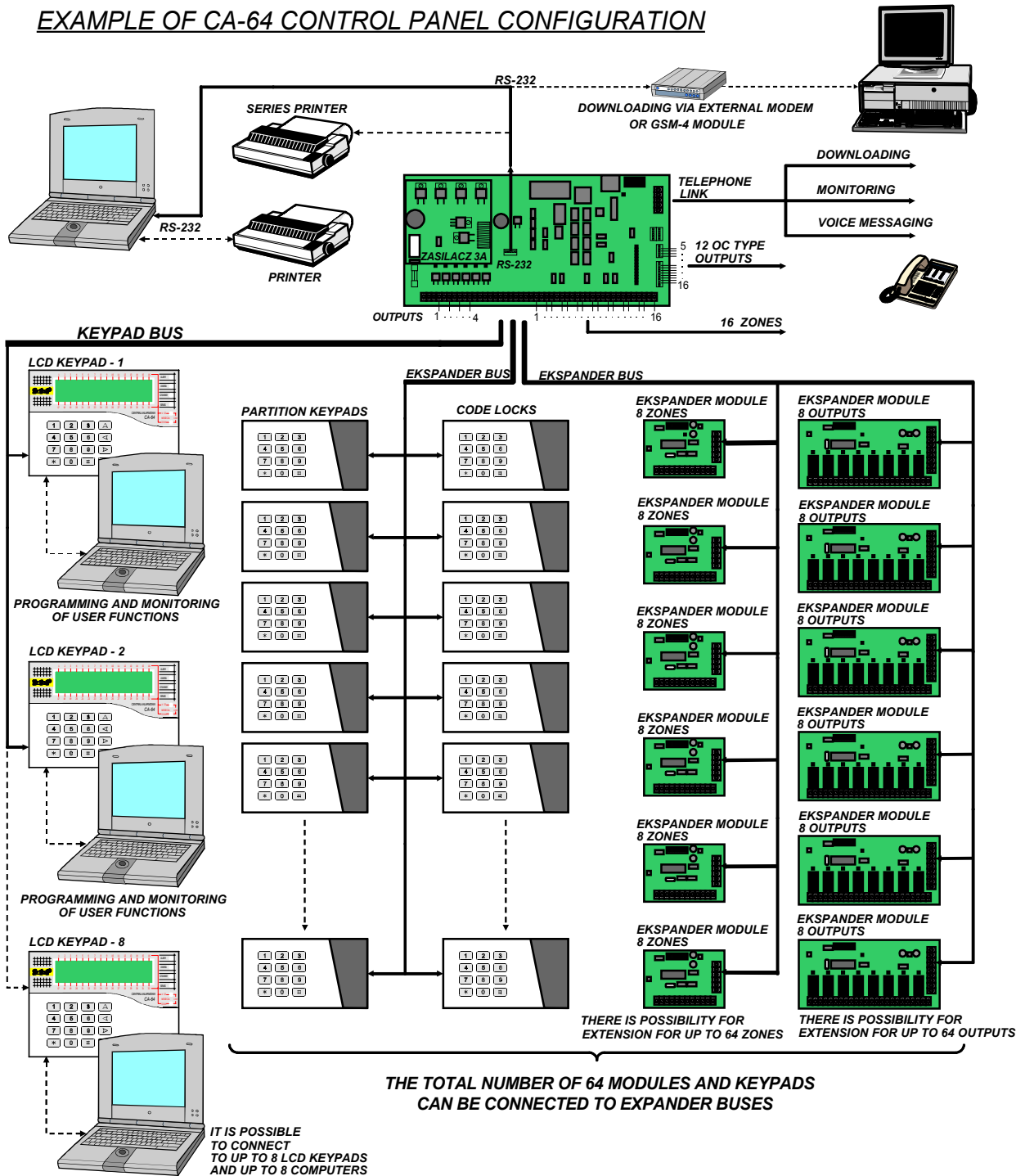
3.11 ADDRESSABLE ZONES EXPANDER

- Bus (3 wires) for connecting up to 48 addressable modules operating with typical detectors, mounted directly in the detector casing; the detector with addressable module mounted inside it is referred to as "addressable detector",
- Additional zone for monitoring the module tampering,
- Switching-mode power supply, output load 2.2 A, with short circuit protection.
- Battery charging and control circuit with disconnecting the discharged battery.

3.12 VOICE SYNTHESIZER EXPANDER

- Memory module for storing 16 verbal messages, 15 seconds per each message.

EXAMPLE OF CA-64 CONTROL PANEL CONFIGURATION



4. FUNCTIONAL DESCRIPTION

In this section, basic information on CA-64 control panel features is given, as defined in the firmware stored in FLASH memory. Views of the DLOAD64 program windows (version 1.04.04) are used in the system descriptions.

4.1 OBJECTS

The CA-64 control panel makes it possible to create up to 8 objects. The objects are created in the service mode by using the „Edit object” function. They are treated as separate alarm systems. It is possible to configure the control panel so that either individual objects have their own separate controls (LCD keypads, partition keypads, code locks) and signaling units, or they share the hardware.

In the case of common LCD keypads, the code of the user giving command defines the object controlled (keypads are not “connected” to partition, GOTO type functions are not needed).

Events from individual objects are sent to the monitoring station with individual identifiers. After selecting the Ademco Contact ID format, the control panel sorts the events automatically. For other formats, the service personnel assign the events to identifiers, according to the assignment of system components (zones, partition, users) to individual partitions.

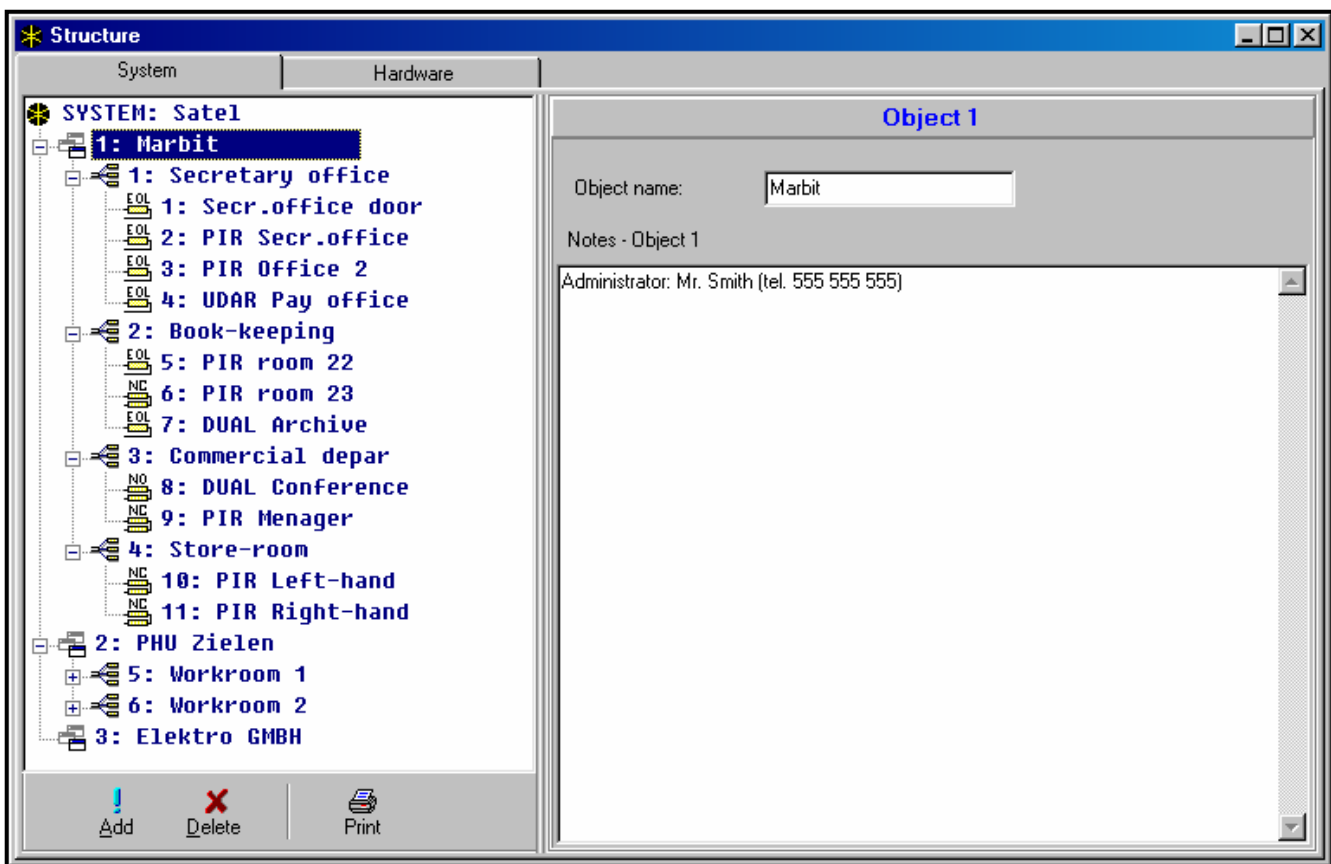


Fig. 1. System division into objects and partitions.

4.2 PARTITIONS

The partition is a **group of zones** for supervising the selected separate part of object, which are armed or disarmed at the same time. Division of the object into partitions improves object security (some object partitions may be armed while the other have been already disarmed), and permits to restrict the users' access to some parts of the facility. For example, in the facility shown in Figure 1, the workers of Commercial Department (partition 3) will not enter the book-keeping rooms (partition 2), unless they are granted authorization to arm / disarm the “Book-keeping” partition.

A partition can be created in the service mode by means of the „Edit object” function, by assigning it to the selected object. When creating a partition, it can be given a **name** (up to 16 characters). Also, the **partition type** should be defined (by default: *Armed with code*).

The CA-64 control panel makes it possible to create a few types of partitions:

- **Partition armed with a code** – basic partition type. Arming and disarming is done by the user. Partition of this type is provided with a timer of its own to arm and/or disarm it, if this was not done earlier by the user.
- **With temporary blocking** – it is a version of the above described type of partition. The difference is that at the time of arming the control panel asks for the blockage time period. Disarming of this partition is possible only after the blockage time period elapses. Disarming may be done before the blockage time period is up only by using a code with „access to temporary blocked partitions” authority, as well as by another code, if an alarm occurred in this partition.

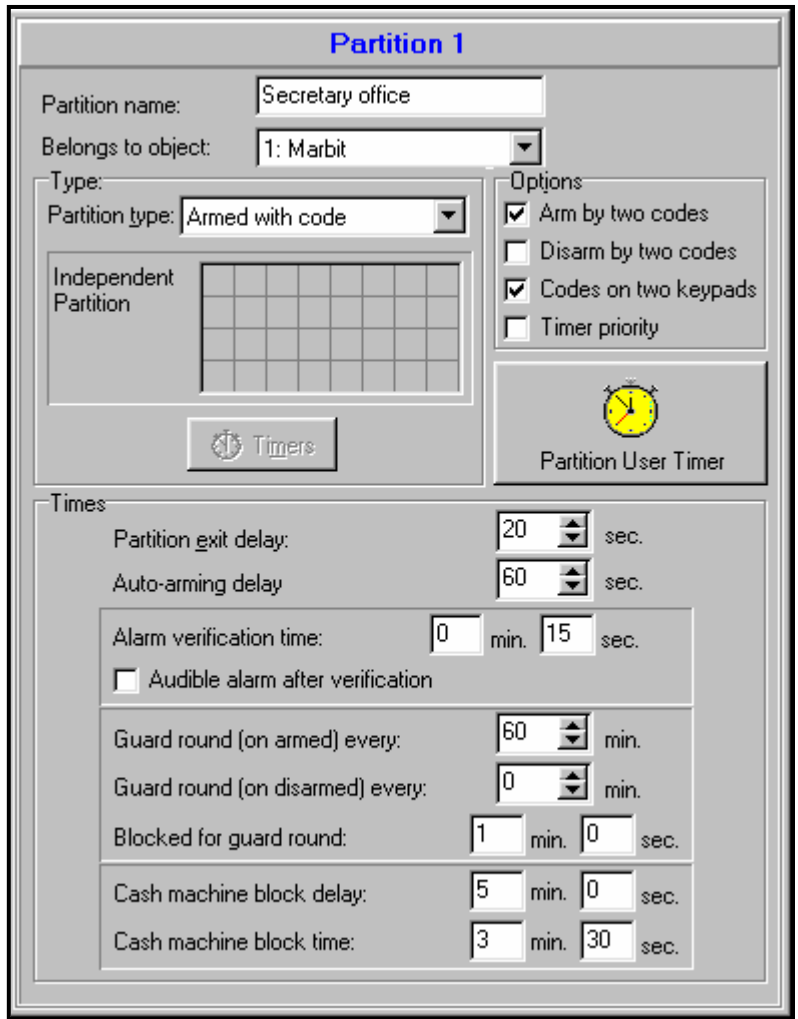


Fig. 2. Partition settings

- **Follow type "AND"** – the partition controlled by statuses of other partitions. Arming for this partition is not done directly by the user, but automatically – when all partitions indicated to the control panel become armed. The list of partitions is defined by the service when creating the dependent partition. The time of dependent partition arming is recorded in the event log, indicating the user who armed the last partition from the list. When any partition from the list is disarmed, the dependent partition will be disarmed as well. Figure 3 shows the selection field of partitions that control partition 3 (partitions 1 and 2 are selected, other colors of background for partitions 3 and 4 show that partitions 3 and 4 cannot be selected for controlling the dependent partition) For *Follow type "AND"* partition no exit delay is defined – the moment of switching over from “exit delay” to “armed” for this partition is set by the last partition from the control list entering the armed status. The dependent partitions cannot be controlled by timers.

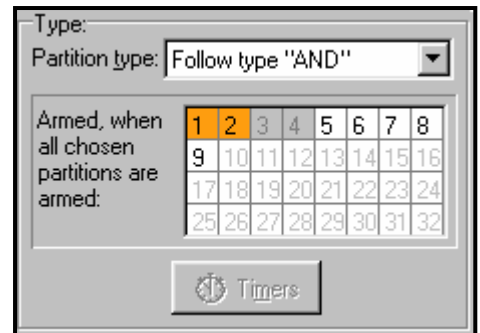


Fig. 3. Definition of *Follow type "AND"* partition.

Note: *Follow type "AND" partitions are usually used for protection of common corridors.*

- **Follow type "OR"** – the partition enters the armed status when any partition from list of control partitions is entering the armed status. The partition is disarmed at the moment

when the last partition contained in the list is disarmed. The exit delay time is the same as for the controlling partition which causes arming of the *Follow type* "OR" partition.

- **Access according to timer** – the partition is controlled by the user, but partition arming and disarming may be carried out only within time periods determined by selected timers. The partition cannot be armed or disarmed in time periods other than those determined by timers. For example, if the timer shown in Figure 4 is selected to control access to the "Secretary office" partition, the partition arming / disarming will be possible according to schedule – on Monday between 16:30 and 16:45, on Friday between 18:00 and 18:15 and so on, except for the time periods given in the timer exception table.

Note: The „access to temporary blocked partitions" authority allows the user to freely control the partition armed mode, irrespective of the timer status.

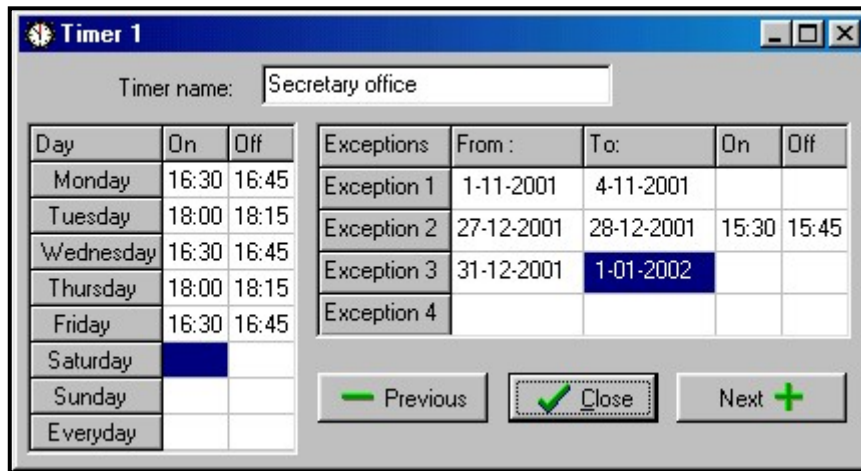


Fig. 4. Timing for *Steered by timer* partition.

- **Steered by timer** partition – the partition, which is armed in time periods determined by selected timers, and may also be controlled by the user code. When creating the *Steered by timer* partition, you should specify the list of timers which determine the periods when the partition is armed. 32 timers may be selected. The control panel analyzes the status of timers selected, and, if any timer status changes to "ON", the control panel arms the partition. Exit delay time is counted-down before entering the full armed status. The partition is disarmed when all timers selected are "OFF". The partition can be also controlled by means of a separate "**Partition user timer**", whose mode of operation is programmable through the user function "*Change option*". The timer controls the partition independently of the other timers. This way of controlling the partition armed status is closely connected with the „**Timer priority**" option.

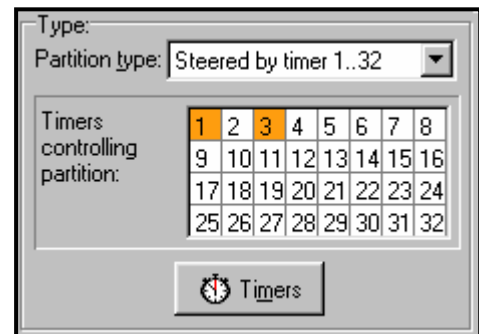


Fig. 5. Selection of partition controlling timers.

Note: When the partition is armed by the timer, the "Automatic arming" event is recorded. The timer number is included in the event. The "0" number indicates that the user timer armed the partition.

The following **options** and **time settings** may be programmed for the partition:

- **Arm by two codes** - arming after entering in succession of two different codes authorized to control the partition.
- **Disarm by two codes** - disarming after entering in succession of two different codes authorized to control the partition.

Codes on two keypads - enabling this option will not allow codes to be entered from the same keypad (which applies to arming/disarming by means of two codes).

Timer priority - when this option is selected, the timer will always perform arming and disarming according to the programmed times. With this option deselected, the disarming only follows if the arming was performed by timer - if the user sets armed mode with a code, the timer will not disarm the partition.

EXAMPLE: If the partition is armed/disarmed by timer every day, and the user is leaving and wants the armed mode to be on for a longer period of time - he will arm the partition himself. With the "timer priority" option disabled, the timer will not disarm the partition at the preset time and the user will not have to remember blocking the timer. When the user comes back and disarms the partition by using the code, the automatic control of the partition is restored according to the timer settings.

Partition user timer – see: **Steered by timer partition** (for the DLOAD64 program the function is available only when making connection to the control panel).

Partition exit delay - delay before the partition is armed.

Auto-arming delay - the time by which the **timer** will delay the automatic arming of a partition. Countdown of this time may be indicated on the partition keypads, LCD keypads and on the control panel outputs. Entering a value bigger than zero will enable an additional menu, which makes it possible to delay auto-arming (by entering a delay time). During the auto-arming countdown it is possible to block the auto-arming function (until the next auto-arming time) by entering zeros alone in the *Defer auto-arm* user function.

Alarm verification time - if in the partition contains zone with "**prealarm**" option on, then panel will trigger alarm from this zone only if during Alarm Verification Time any other zone will be violated.

Audible alarm after verification - enabling the option means that there will be no audible signaling of prealarm, i.e. violation of the zone with prealarm option on - the audible signaling will only be triggered when another zone is violated during the alarm verification time.

Guard round (on armed) every

Guard round (on disarmed) every

Blocked for guard round

If the facility is watched by a **guard**, the round monitoring and signaling of guard absence in specified time is possible – when the guard enters his code from an LCD, partition or code lock; this is registered in the memory of events. The related times are declared separately for each partition; programming the "0" time disables the monitoring function. It is possible to differentiate monitoring times depending on whether the partition is armed or not. When the partition round requires violation of detectors and the guard is not authorized to switch the detectors off, it is possible to program the bypass time period, which starts when the guard enters his code to make a round. Also, partition bypass may be activated by entering the code like "Temporary partition bypassing".

Cash machine block delay

Cash machine block time

Times are programmable if the system supervises the cash dispensers by means of the 24H CASH MACHINE zones. Each partition may contain one cash point only. Access to the cash point is possible after entering the "Access to cash dispenser" type of code from LCD keypad (or computer). This bypass starts the "time for approaching" the cash point (24H CASH MACHINE zone is still armed), and, afterwards, the bypass time period is counted down (during the countdown 24H CASH MACHINE zone is bypassed).

4.3 ZONES

The zone input in the alarm system is the interface of mainboard, LCD keypad or expansion module. Two electrical wires, or the so-called "**line**", are to be connected between the input terminal and the ground, the line being terminated with an alarm detector or another type of sensor. Along with the detector, the resistor may also be included in the electric circuit (1 or 2, depending on the detector type).

4.3.1 IDENTIFICATION AND NUMBERING OF ZONES IN THE SYSTEM

The number of available (existing) zones is recognized by the control panel in the process of expansion module identification. Therefore, prior to partition programming, it is necessary to:

- carry out the security system installation,
- perform identification of keypads and expanders (using functions available from the control panel LCD keypad in the service mode),
- when the control panel is programmed by means of computer - download the data from the control panel to the computer,
- perform logical partitioning of the system (creating additional objects, assigning partitions to the objects),
- assign zones to the created partitions.

Notes:

- *After restart of the settings (also in the new control panel), most of the service mode functions are not available until the control panel completes identification of hardware.*
- *The control panel will automatically assign numbers of the system zones to those of the mainboard and expanders (see instructions „CA-64 E Zone Expander“). The sequence of zone assignment depends on the addresses set at the expanders. The mainboard zones always carry the numbers from 1 to 16.*
- *The expander of addressable zones cannot be installed together with other zone expanders. Identification of the addressable zones (e.g. after adding some zones in the system) is carried out jointly with expander identification.*
- *On the LCD keypad, the expander addresses in the name programming function are given in hexadecimal format in the following manner:*
 - *addresses from 00 to 1F refer to the first expander bus (the numbering corresponds to the addresses set at microswitches – default names: **Expander 01 ... Expander 32**)*
 - *addresses from 20 to 3F refer to the second expander bus (continuation of the first bus addresses calculated as: microswitches setting +32 (20 in hexadecimal format) default names: **Expander 33 ... Expander 64**).*
- *The same zone cannot be assigned to several partitions at the same time. However, it is possible to create partitions dependent on the status of other selected system partitions.*

Suitable parameters and options should be programmed for each zone:

4.3.2 PARAMETERS

Zone name - up to 16 characters

Assigned to partition

Zone type

Entry delay / Alarm delay / Signaling delay / Surveillance time / Bypass time

Expander number – refers to type 58 zones: TECHNICAL - DOOR BUTTON.

Arming mode - the following armed modes are to be selected for type 80 & 82 zones:

- 1– normal armed mode;

2– INTERIOR DELAYED zones (type 3 zones) will be bypassed, EXTERIOR (type 8 zones) will trigger silent alarm, and the other ones - audible alarm;

3– same as 2, but, the type 0, 1 & 2 DELAYED zones will act as instant ones.

Detector configuration – configuration of the connected detector (NO, NC, EOL etc.). The CA-64 control panel enables lines terminated with any detectors to be connected to the zones in the following configurations (see: „*Connection of detectors*” p. 45):

NC (detector with normally closed output),

NO (detector with normally open output),

EOL (detector in configuration with end of line resistor),

2EOL/NO (NO type detector in configuration with double end of line resistor),

2EOL/NC (NC type detector in configuration with double end of line resistor).

Zone sensitivity - the necessary duration of the actual zone violation until it is recorded by the control panel (typically approx. 0.5 sec., e.g. for the PANIC button a shorter time is recommended).

Fig. 6. Details of zone settings.

Max. violation time / Max. door opening time – exceeding the maximum time of violation / door opening is recognized by the control panel as a detector failure (e.g. damaging or masking the detector) / door. The „0” value will deactivate the time control.

Max. no violation time - exceeding the maximum time of no violation is recognized by the control panel as a detector failure (e.g. damaging or masking the detector). The „0” value will deactivate the time control.

4.3.3 OPTIONS

Power up delay - the zone will be bypassed for 120 sec. after power is switched on (which prevents triggering alarms e.g. when starting the alarm control panel).

Priority - this option makes arming impossible, if the zone with activated option is violated (e.g. in case when windows have been left open, etc.).

Note: *Prior to arming you can preview the names of violated zones for which the „Priority” option has not been activated. To do so, select the „Zones bef. arm” (→Service mode →Options →Various options).*

- Disarm on violation** – option for type 82 zone - consecutive violations of the zone alternately arm / disarm the partition. If the option is not selected, zone violation will arm and end of violation will disarm the partition.
- Chime (on outputs)** - violation of the zone will activate the CHIME type output.
- Video On Disarmed** - violation of the zone will activate the VIDEO ON DISARMED type output (intended for starting cameras and video recorders).
- Video On Armed** - violation of the zone will activate the VIDEO ON ARMED type output (intended for starting cameras and video recorders).
- Bypass disabled** - the zone cannot be bypassed by the "zone bypass" user function.
- Bypassed if no exit** - the zone will be automatically bypassed, if during the zone exit delay no detector (zone) of the ENTRY/EXIT or EXIT type is violated.
- Alarm if armed** – option available to type 64-79 zones, when the „**No bypass in armed**” option is selected. Violation of the zone when the partition it belongs to is armed will trigger an alarm.
- Auto Reset 3** - the zone will be automatically bypassed if 3 alarms have been triggered since arming time.
- Auto Reset 1** - the zone will be automatically bypassed if 1 alarm has been triggered since arming time.
- Clearing Autoreset** - if option is on, and zone has Auto Reset 1 or Auto Reset 3 option on and the zone was automatically bypassed, the panel will clear the bypass once every 24h, at midnight.
- Prealarm** - zone with alarm verification.
- Bell delay** - the zone triggers alarm instantaneously (starts monitoring and telephone messaging), but audible signaling will be delayed by the time set as the "entry delay".
- Alarm if armed** - option available to type 64-79 zones, with the „No bypass in armed” option selected – an attempt to bypass the zone in armed mode will trigger an alarm.
- Clear alarm** – option available to type 81 & 82 zones. Violation of the zone will clear alarm in the partition, if it is currently indicated.
- Abort delay** - information on the zone violation will not be reported to the monitoring stations if the violation occurred during the entry time.
- Partition temporary blocking** – option for the type 84 zone. Violation of the zone will block the partition for the time of guard round.
- Restore after bell** - the zone violation end code will be reported to the monitoring station not immediately but after alarming is over.
- Restore after disarm** - the zone violation end code will be reported to the monitoring station not immediately but only after the alarm is cleared and the zone disarmed.
- Alarm on Exit delay end** - the zone will trigger alarm if at the moment of the exit delay time elapsing it is in the state of violation (with this option disabled the alarm is triggered only if the zone state changes from normal to violation - when armed).
- Write violations to event log** - option for the type 47 zones: NO ALARM ACTION – each zone violation will be recorded in the event log.
- No bypass in armed** – option for the type 64-79 zones. Violation of the zone when the partition it belongs to is in armed mode will block no group of zones.
- Abort voice messaging** – option for the type 81-83 zones. Violation of the zone will cancel the messaging, if it is currently underway.
- Alarm on unbypass** – the zone will trigger an alarm if it is violated after unbypassing, and the partition is armed.

4.3.4 ZONE TYPE

- 0. ENTRY/EXIT** - delayed zone combining two functions:
- entry** - violation of the zone starts entry delay counting in the partition and turns on delay for the Interior delayed zones; the entry time may be signaled on keypads;
 - exit** - during the exit delay the panel keeps watching the zone for violation - in case of no violation (the user has armed the zone but not left the facility), the zones with the "bypassed if no exit" option active will be bypassed.
- 1. ENTRY** - see the ENTRY/EXIT zone.
 - 2. DELAYED WITH DELAY SIGNALING** – a delayed-action zone with optional signaling of counting delay in keypads.
 - 3. INTERIOR DELAYED** - conditionally delayed zone: delay is only activated when the ENTRY or ENTRY/EXIT zone has been violated first.
 - 4. PERIMETER** - instantly armed zone, allowing no time for exit.
 - 5. INSTANT** - instant burglary zone, without additional functions.
 - 6. EXIT** - see the ENTRY/EXIT zone.
 - 7. DAY/NIGHT** - if disarmed, the zone will signal violation acoustically in keypads and on the ALARM DAY type outputs (signaling for a time period preset for the given output); when armed, the zone acts as the INSTANT zone
 - 8. EXTERIOR** – a zone with alarm verification: violation of the zone will start counting the observation time (programmed as the zone entry delay) - if a second violation takes place during this time, an alarm will be triggered. The first violation may be signaled at the ALARM DAY type output.
 - 9. 24H TAMPER** - permanently armed zone, intended for the tamper circuits.
 - 10. 24H VIBRATION** - 24h zone intended for working with vibration detectors: during arming (from LCD keypad), an automatic test of these detectors is performed - prior to starting the „exit delay” countdown, the VIBRATION DETECTORS TEST type output is activated and countdown begins of testing time, during which all vibration type zones in the given partition should be violated.
 - 11. 24H CASH MACHINE** - zone intended for protection of a cash machine (see: Partitions).
 - 12. PANIC-AUDIBLE** - permanently armed zone, intended for operating the panic buttons.
 - 13. PANIC-SILENT** - permanently armed zone, violation of which starts reporting to the monitoring station and activates the SILENT ALARM type outputs without activating the audible alarm signaling.
 - 14. MEDICAL - BUTTON**
 - 15. MEDICAL - REMOTE CONTROL** - violation of the medical zones will trigger an alarm signaled in keypads and on the SILENT ALARM type outputs. The names of zones and the codes of events from those zones are compatible with the Ademco Contact ID monitoring standard.
 - 16÷31 COUNTING L1÷16** – the counting zones will signal an alarm when the number of violations counted during a specified time period exceeds the set value. The control panel offers the possibility to program 16 different counters, which define how the counting zones will operate. Several zones can be assigned to each counter, thus creating a group of counting zones. Violations of the counting zones in armed mode can be signaled at the ALARM DAY type output.
The following is to be programmed for each group of counting zones (counters):
 - Max. value - number of zone violations which, if exceeded, will trigger the alarm,
 - Counting time - the time in which violations are counted,
 - Counter type
 - *normal*: all violations of counter group lines are counted,

- *omits recurs*: consecutive violations of the same zone are not counted (alarm will be triggered if the number of violations from different zones exceeds the maximum value).

32. 24H FIRE**33. 24H FIRE – SMOKE****34. 24H FIRE – COMBUSTION****35. 24H FIRE – WATER FLOW (FIRE)****36. 24H FIRE – HEAT****37. 24H FIRE – BUTTON****38. 24H FIRE – DUCT****39. 24H FIRE – FLAME**

All the fire zones (type 32÷39) trigger alarms signaled on the FIRE ALARM type outputs. They differ in the alarm code being sent to the monitoring station in the Ademco Contact ID format. The names of these zones are compatible with the names of event codes in the CID format. The fire outputs (except for the 24H FIRE – BUTTON) can work with alarm verification.

40. 24H FIRE SUPERVISORY**41. 24H LOW WATER PRESSURE****42. 24H Low CO2****43. 24H WATER GATE DETECTOR****44. 24H LOW WATER LEVEL****45. 24H PUMP ACTIVATED****46. 24H PUMP FAILURE****47. No ALARM ACTION** - zone intended for activating the outputs (e.g. ZONE VIOLATION, READY STATUS etc.). If option "Write violations to event log" is on for this zone, every violation will be recorded in the event log.**48. 24H AUXILIARY – PROTECTION LOOP****49. 24H AUXILIARY - GAS DETECTOR****50. 24H AUXILIARY - REFRIGERATION****51. 24H AUXILIARY - LOSS OF HEAT****52. 24H AUXILIARY - WATER LEAKAGE****53. 24H AUXILIARY - FOIL BREAK****54. 24H AUXILIARY - LOW BOTTLED GAS LEVEL****55. 24H AUXILIARY - HIGH TEMPERATURE****56. 24H AUXILIARY - LOW TEMPERATURE****57. TECHNICAL - DOOR OPEN** - zone intended for supervising the status of the door defined as the *Dependent door* in the access control module (which controls the door electromagnetic lock).**58. TECHNICAL - DOOR BUTTON** - zone intended for opening the door controlled via a partition keypad, code lock (or another access control module). The value of entry delay time entered for such a zone means the address of a door control module (from 0 to 31 – modules of 1 bus, from 32 to 63 - modules of 2 bus, 32 - address 00, 33 - address 01, etc.). Violation of such a zone will switch over the selected module relay and open the door (e.g. entering a room requires the access code to be entered on the keypad installed outside the door, while for exiting it is enough to press the button situated at the door inside the room).

- 59. TECHNICAL - AC LOSS** - provided for control of the devices interacting with the alarm control panel e.g. additional power supply units. Violation of this zone will trigger the trouble alarm on the control panel.
- 60. TECHNICAL - BATTERY LOW** - intended for the battery control in additional power supply units working with the control panel. Violation of this zone will trigger the trouble alarm on the control panel.
- 61. TECHNICAL - GSM LINK TROUBLE** - intended for control of the external GSM communication module. Violation of this zone will trigger the trouble alarm on the control panel.

The zone types from 40 to 61 (auxiliary and technical) signal alarms on the Technical alarm type outputs. The names of zones and the codes of events from those zones are compatible with the Ademco Contact ID monitoring standard.

62,63. RESERVED

64÷79 BYPASSING - GROUP: 1÷16 - violation of this type of zone will bypass a specified group of zones. The control panel enables up to 16 zone groups to be defined. The group is created by selecting the zones and defining how they will be bypassed:

- *Bypass only* - violation of the zone bypassing a particular group will bypass the zones. If the bypassing zone has a fixed "entry delay" time, the group will be bypassed for such a time. If the "entry delay" time for that line is equal to zero, unbypassing of the group will follow automatically when the partitions to which the zones belong are disarmed.
- *Bypass on/off* - violation of a bypassing zone will bypass the zones, while end of violation will result in unbypassing the same.

Additionally, the following **options** are available to this type of zone:

- **No bypass if armed** - when this option is enabled, the zone will be bypassed, provided that the partition it belongs to is armed.
- **Alarm in arm state** - with this option enabled, violation of the bypassing zone in the armed mode will **trigger an alarm**.

- 80. ARMING** - violation of the zone will arm the partition to which the zone belongs.
- 81. DISARMING** - violation of the zone will disarm the partition to which the zone belongs, and can also clear the alarm and cancel the messaging.
- 82. ARM/DISARM** - the zone controls the arming status of the partition it belongs to. Additionally, activating the Controlled when armed option enables the user to choose the control mode:
- option deactivated: violation of the zone will arm, and end of violation will disarm the partition ("switch"),
 - option activated: consecutive violations will arm/disarm the partition ("switch").
- Disarming may simultaneously clear the alarm and cancel the messaging.
- 83. CLEARING ALARM** - violation of the zone will clear alarm in the partition to which the zone belongs, and can also cancel messaging.
- 84. GUARD** - violation of the zone is treated as recording the guard's round in the partition to which the zone belongs.
- 85. ENTRY/EXIT - CONDITIONAL** - ENTRY/EXIT zone with additional feature: if user arm the system without leaving protected area (without violating of this zone during *exit delay*) the zone will work as INSTANT zone - with no entry delay.
- 86. 24H BURGLARY** - a permanently armed zone, violation of which will trigger a burglary alarm.

4.4 OUTPUTS

The control panel outputs are intended for switching on and off the external devices (signaling, lighting, air conditioning, etc.) connected to corresponding terminals of the mainboard or expander. Each of the outputs can serve one of a few dozen functions or can be activated through a combination of other outputs functions (the *Logical AND* and *Logical OR* type of outputs). Triggering sources for each output are defined separately. All the outputs (in mainboard and/or expanders) are fitted with LEDs to indicate their current status. The numbers of system outputs are determined in much the same way as the zone numbers. The outputs not assigned to expanders can be used to perform logical functions.

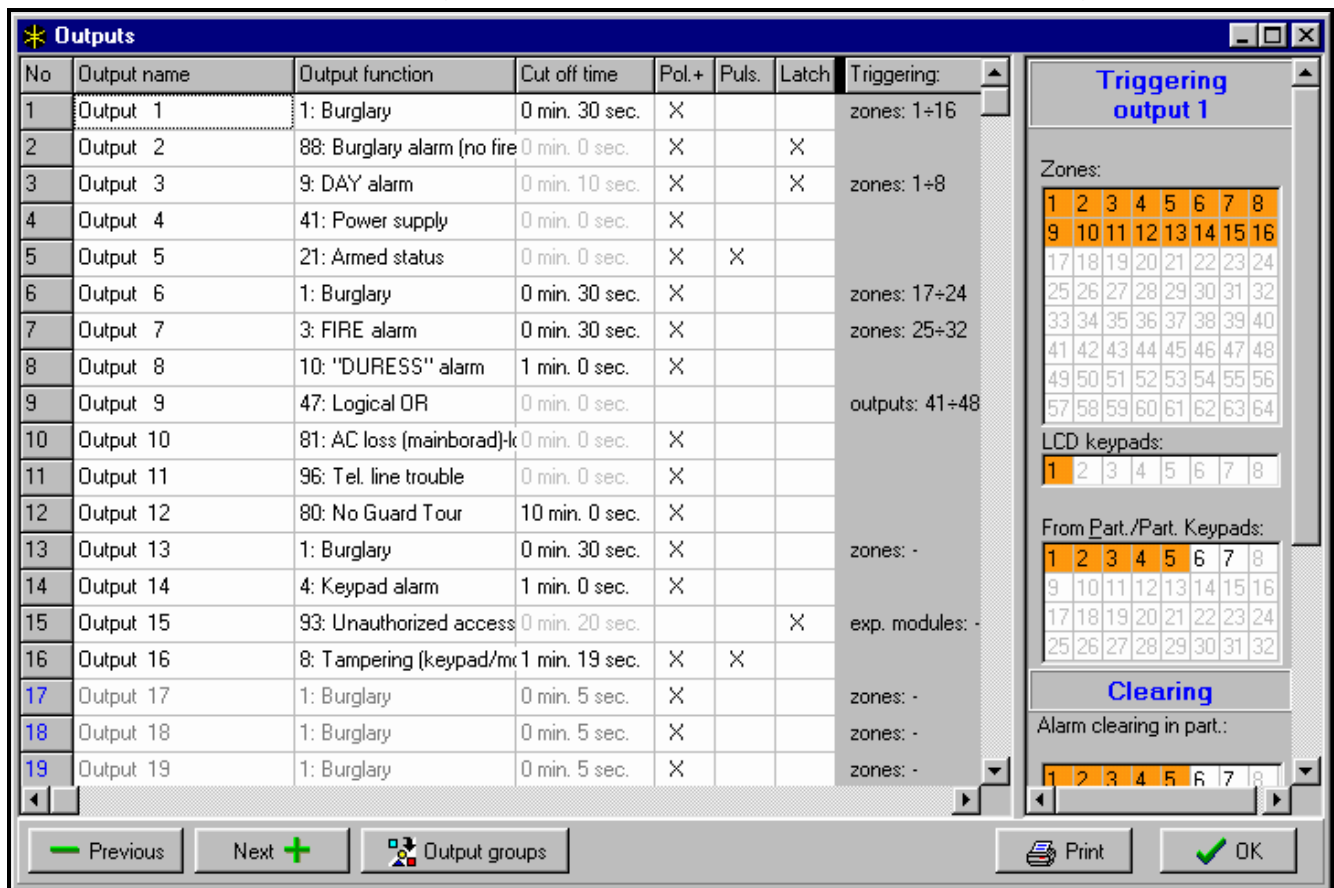


Fig. 7 Details of output settings.

Suitable parameters and options should be programmed for each output:

4.4.1 PARAMETERS

Output name - up to 16 characters.

Output type (see the list of *output types*)

Cut off time – refers to the outputs responding to events (alarm, video control outputs, etc.), for the status indicating ones this time is irrelevant.

4.4.2 OPTIONS

Polarization – determines whether 12V or 0V (common) is to be at the active output,

- for high-current outputs: active state +12V, inactive state 0V (ground);
- for OC type outputs: active state - shorted to the ground; inactive state - cut off from the ground.

Note: If the option is not set (selected) the output will act in the opposite way.

Pulsation - determines if the output signal is to be continuous or pulsating (0.5/0.5 sec.) - the option only applies to the timed outputs;

Latch - (refers to the alarm outputs only) when this option is active, the output will be operative until alarm is cancelled by entering the code.

4.4.3 SOURCE OF OUTPUT TRIGGERING

Depending on its type, the output can be triggered in various ways. The control panel makes available selection lists for triggering sources suitable for particular types of outputs. For example, you can program zones, keypads, partitions/partition keypads to control zone for the alarm outputs; master users (administrators) and users for the CODE ENTERED SIGNALING/CODE USED SIGNALING outputs; control timers for the TIMER type outputs, etc.

Triggering from zones – enables the user to select any number out of the 64 zones which will cause activation of the output.

Triggering from LCD keypads – refers e.g. to the alarms called from keypads and permits determination which outputs will react to those alarms.

Triggering from partitions / partition keypads – refers to the alarms in partitions and those called from partition keypads, including the keypad tamper alarms.

Triggering from control timers – provides option to select any timers which are to activate the output.

Triggering by administrators – refers to the administrator codes which will activate the output.

Triggering by users – refers to the user codes which will activate the output.

Triggering from control outputs – refers to the outputs, the activation of which will affect the particular output status.

Triggering from expansion modules – makes it possible to define which expanders will activate the output.

Triggering by telephone line trouble – makes it possible to select the type of failure to be signaled at the output.

Triggering from reset zones - makes it possible to indicate zones which will temporary disable the output (verification of fire alarms).

4.4.4 CLEARANCE AVAILABILITY

Alarm canceling - the list of partitions makes it possible to determine which event will disable the output: an alarm will only be canceled if the alarm signaling is canceled in one of the selected partitions.

Note: *Make sure, that the output alarm canceling is assigned to the partition which triggers that output – otherwise, it will be impossible to cancel alarm at that output since the canceling partition will not be signaling any alarm.*

4.4.5 OUTPUTS TYPE

0. NOT USED

1. **BURGLARY ALARM** - signals all burglary and panic alarms (from zones, keypad / expander tamper, keypad Panic, etc.).
2. **FIRE / BURGLARY ALARM** - signals the burglary and panic alarms (continuous sound) and the fire alarms (intermittent sound).
3. **FIRE ALARM** - signals the fire alarms (from fire zones and triggered from keypads).
4. **KEYPAD ALARM** - signals all alarms (fire, panic, auxiliary alarm, 3 bad codes, keypad tamper).

5. **KEYPAD FIRE ALARM** - signals the fire alarms triggered from keypad (by keeping pressed the [*] key for 3 sec.).
6. **KEYPAD PANIC ALARM** - signals the panic alarms triggered from keypad (by keeping pressed the [#] key for 3 sec.).
7. **KEYPAD AUXILIARY ALARM** - signals the calling medical assistance alarm triggered from keypad (by keeping pressed the 0 key for 3 sec.).
8. **KEYPAD / EXPANDER TAMPER ALARM** - signals the module tamper alarms - module tamper contact open, module non-existent or verification error (detection of a wrong address or module replacement).
9. **DAY ALARM** - signals violation of the DAY/NIGHT type zones when the system is disarmed, or violation of the COUNTING and EXTERIOR type zones before an alarm is triggered.
10. **DURESS ALARM** - signals that a DURESS type code has been used in the system.
11. **CHIME** - signals violation of zones with the chime option on (the user can block the chime signaling from selected partitions by using a suitable function from the user menu; the function can be automatically disabled for a specified time period after violation of the selected zone)
12. **SILENT ALARM** - signals violation of the PANIC-SILENT type zone, from alarm zones with the *Signaling delay option* on, and the calling medical assistance alarms from the MEDICAL-BUTTON and MEDICAL-REMOTE CONTROL
13. **TECHNICAL ALARM** - signals violation of the 24H AUXILIARY zones (zone types 40 - 56).
14. **ZONE VIOLATION** - the output is activated by a violation of selected zones.
15. **VIDEO ON DISARMED** - the output is activated by a violation of selected zones with the *Video on disarmed* option active (the zone is disarmed).
16. **VIDEO ON ARMED** - the output is activated by a violation of selected zones with the *Video on armed* option active (the zone is armed)
17. **READY STATUS** - signals "readiness" of selected zones to be armed (all zones are free from violations)
18. **BYPASS STATUS** - signals that some selected zones have been bypassed.
19. **EXIT DELAY WARNING** - signals that *Exit delay* is running in selected partitions.
20. **ENTRY DELAY WARNING** - signals that *Entry delay* is running for selected zones or in selected partitions.
21. **ARM STATUS** - the output is activated if at least one of the selected partitions is armed.
22. **FULL ARM STATUS** - the output is activated if all of the selected partitions are armed.
23. **ARM/DISARM ACKNOWLEDGE** - signals arming / disarming one selected zone (1 signal 0.5 sec. - arming, 2 signals - disarming, 4 signals - alarm canceling).
24. **MONO SWITCH** - the output is activated for a specified time with a *MONO output control* type code; the output should be assigned to specific partitions and/or zones, and will be activated by a code entered from LCD keypad or partition keypad serving that partition, or when the selected zone is violated.
25. **BI SWITCH** - the output is activated / deactivated by a *BI output control* type code; the output should be assigned to specific partitions and/or zones, and will be activated by a code entered from LCD keypad or partition keypad serving that partition, or when the selected zone is violated.
26. **TIMER** - the output is armed and disarmed by selected timers.
27. **TROUBLE STATUS** - signals detection of a trouble condition (mains power supply failure, low battery, defect of zones, expander buses, etc.).
28. **AC LOSS - CONTROL PANEL MAINBOARD** - signals mains power failure of the control panel mainboard.

29. **AC LOSS (FROM ZONES)** - signals violation of the selected TECHNICAL-AC LOSS type zones.
30. **AC LOSS (FROM EXPANDERS)** - signals mains power failure of the selected expanders with power supply units (expander selection: from 0 to 31 - bus 1 modules, from 32 to 63 - bus 2 modules).
31. **BATTERY TROUBLE - CONTROL PANEL MAINBOARD** - signals low voltage condition of the backup battery of the control panel mainboard.
32. **BATTERY TROUBLE (FROM ZONES)** - signals violation of the selected TECHNICAL-BATTERY LOW type zones.
33. **BATTERY TROUBLE (FROM EXPANDERS)** - signals low voltage condition of the backup battery of the selected expanders.
34. **ZONE TROUBLE** - signals exceeding the *Maximum violation time* or the *Maximum no violation time* of the selected zones.
35. **TELEPHONE USAGE STATUS** - signals that the control panel is on the telephone.
36. **GROUND START** - the output generates a control pulse necessary for work with some types of telephone exchange.
37. **MONITORING ACKNOWLEDGE** - the output activated after successful completion of connection with the monitoring station.
38. **SERVICE MODE INDICATOR** - signals activation of the service mode on one of the control panel LCD keypads.
39. **VIBRATION DETECTORS TEST** - the output intended for testing the vibration detectors in one selected partition (see: Zone types – 24H VIBRATION). The output cut-off time defines the maximum duration of testing the vibration detectors in the selected partition.
40. **CASH MACHINE BYPASS INDICATOR** - signals bypassing the 24H CASH MACHINE type zones in selected partitions.
41. **POWER SUPPLY** - the output intended for supplying the external devices: the zones 1 to 4 of the control panel mainboard (high-current outputs with electronic protection) are recommended to be used as power supply zones.
42. **POWER SUPPLY IN ARMED STATE** - the power supply output is activated on arming some selected partitions (when the exit delay starts) - it is intended for supplying e.g. ultrasound or microwave detectors, or infrared barriers, which should not be enabled if not used by the system.
43. **RESETABLE POWER SUPPLY** - the power supply output resetable from the user menu in LCD keypad. The reset (power cut-off) time for the resetable output is programmed as that output cut-off time.
44. **FIRE POWER SUPPLY** - the output intended for supplying the fire detectors with automatic alarm verification. The verification proceeds as follows: after detecting violation of one of the fire zones assigned to the given output the power supply is cut off (for a time programmed as the output cut-off time) and, in case next violation occurs after power supply is switched on again, the fire alarm will be triggered. The output can be also reset by the use of a suitable user function (as the RESETABLE POWER SUPPLY type output).
45. **PARTITION BLOCKED INDICATOR** - signals that the partition armed state is temporarily blocked. If "cut off time" of this output will be greater than zero, the output will signal the ending of partition blocking: output will be activated for programmed period of time just before partition return to arm state.
46. **LOGICAL AND** – output is activated when all the outputs selected as the control ones are active.

- 47. LOGICAL OR** - output is activated when at least one of the outputs selected as the control ones is active. An output is considered to be activated when it is energized with +12V voltage - which allows the output Polarization option to be used as logical negation.
- The CA64 control panel handles 64 outputs, irrespective of whether any extension modules are connected, which physically bring out the activation / deactivation status of a given output. This enables any number of the 64 outputs to be used as the control outputs of the LOGICAL AND or LOGICAL OR type output (see: →the DLOAD64 program →HELP – examples of outputs programming).
- 48÷63 VOICE MESSAGE 1÷16** - the outputs activated by the telephone messaging function: it enables using any external device for playback of notification messages (when programming notification one should select the message number from 1 to 16 thus activating the appropriate output).
- 64÷79 REMOTE SWITCH 1÷16** - the output to be controlled via the telephone line by the *Telephone control* function.
- 80. NO GUARD ROUND** - signals the lack of entering the guard code within the time designated for rounds in selected partitions.
- 81. LONG AC LOSS - MAINBOARD** - signals the mains power supply failure of the control panel mainboard with delay programmed as *Max. AC loss time* (Options - Global times).
- 82. LONG AC LOSS - MODULES** - signals the mains power supply failure of the selected extension modules (modules with power supply) with delay programmed as *Max. AC loss time* for each of the modules.
- 83. OUTPUTS OFF** - the output is activated when all the selected outputs have been deactivated (the signaling is completed).
- 84. CODE ENTERED SIGNALING** - the output is activated on entering the code of a selected user (and pressing the [*] or [#] key).
- 85. CODE USED SIGNALING** - the output is activated on arming or disarming the system, using the code of one of selected users.
- 86. DOOR OPEN INDICATOR** - the output is activated on opening the door supervised by the selected modules of access control.
- 87. DOOR OPEN TOO LONG INDICATOR** - the output is activated on exceeding the maximum opening time of the door supervised by the selected modules of access control.
- 88. BURGLARY ALARM (NO TAMPER OR FIRE ALARMS)** – the output only signals the alarms from armed zones and the PANIC alarms from partition keypads and LCD keypads.
- 89. EVENTS MEMORY 50% FULL** - the output signals that the events memory area has been filled up to 50% (approx. 3000 events) since the last events readout using the DLOAD64 program. The output remains active until the event memory readout.
- 90. EVENTS MEMORY 90% FULL** - the output signals that the events memory area has been filled up to 90% since the last events readout using the DLOAD64 program.
- 91. PARTITION AUTO-ARM DELAY COUNT SIGNALING** - the output becomes active (for a specified time) on starting *auto-arming delay* countdown for the selected partitions.
- 92. PARTITION AUTO-ARM DELAY COUNT INDICATOR** - the output indicates the fact of *auto-arming delay* countdown for the selected partitions.
- 93. UNAUTHORIZED DOOR OPENING** – the output becomes active when the doors supervised by selected access control modules (partition keypads, coded locks, transponders) are opened without access authorization (i.e. without entering the code or reading in the proximity card).
- 94. ALARM - UNAUTHORIZED DOOR OPENING** – the output works in the same way as the type 93 output but only for the modules with the *Alarm when no authorization* option activated.

- 95. PROXIMITY CARD USED SIGNALING** - the output is activated reading the proximity card of a selected user
- 96. TELEPHONE LINE TROUBLE** - the output signals the state of:
- 1 - no voltage on tel. line.
 - 2 - wrong dial tone
 - 3 - no dial tone
 - 4 - Monitoring Station 1 trouble
 - 5 - Monitoring Station 2 trouble
- 97. TAMPER ALARM** – signals tamper alarms.

4.5 CODES AND USERS

Control panel operation (arming and disarming, resetting of alarms and access to functions) is possible after entering the code assigned to the user. The code identifies the user, his authority level in the system and access to partitions and selected parts of the facility (the access is controlled with locks controlled by the CA-64 control panel).

The CA-64 control panel recognizes three code types:

1. **Service codes** – this code identifies the user with special rights: he controls all partitions, he can open all doors controlled by the control panel, he has access to all functions (except “Service access” function, which appears in function menu for the **administrator** only). The code is stored in the EEPROM memory, therefore, it is not lost after removing the 3.6V battery jumper (memory of settings and memory events backup) when the control panel is not powered.
2. **Administrator (supervisor) code** – this code identifies the user with authorization rights given by the service, except for the rights of access to the “Service access” function, which always is accessible to the administrator. If a number of objects is defined in the system, each objects has its own administrator code. Administrator codes are stored in the EEPROM memory.
3. **User code** – the other codes entered in the system by service or administrators, stored in RAM memory with battery backup. These are the codes for everyday operation of the system. 192 user codes may be entered in the CA-64 control panel.

Note: *Taking into account safety of the system (the code may be seen by unauthorized persons), it is recommended that for everyday use the administrators be assigned a code from the group of user codes, with appropriately limited authority.*

The user is entered in the system by calling the “New User” function. The following is determined there:

- **Code** – the code assigned to a new user (if the user is provided with rights to change his code, he should change his code!).
- **Telephone code** – the code for user identification when he use the function **answering the phone call**. If the user is not assigned with this code, he be not able to check statuses of his partitions and control the REMOTE SWITCH type outputs by telephone.
- **Partitions** – partitions which may be accessed by the user (he can arm / disarm them and reset alarms in them). The list of partitions shown in this function is limited to the partitions accessible to the user who enters a new user. When the service enters a user, the system asks about the user object before selecting the partitions.
- **Type** – definition of additional properties of the code:
 1. **Normal** – the basic type of access code assigned to the user.
 2. **One-time** – the access code for single use.

3. **Time renewable** – the access code whose validity time is determined when creating a user. Before expiry of the validity time, the control panel reminds the access code user of the necessary code change, after which the validity time is counted anew. In the duration item of such a user, it is necessary to determine the number of days of the access code validity.
 4. **Time not renewable** – the access code whose validity time is limited to the number of days entered when creating the user. In the duration item of such a user it is necessary to determine the number of days of the access code validity. The validity time can be changed by the user who has introduced the given user type, or by the administrator.
 5. **Duress** – code similar to normal user type, but the use of this code generates additional event, which is sent to monitoring station (“Alarm – forced activity”) and activates an alarm on the DURESS ALARM type outputs.
 6. **MONO output control** – code that switches on outputs of MONO SWITCH type assigned to partitions covered by this code.
 7. **BI output control** – code, which changes the status of outputs of the BI SWITCH type assigned to partitions covered by the code.
 8. **Temporary partition bypassing** – code, which activates the temporary partition bypass (during the bypass period, although the partition is armed, the violation of partition zones will not trigger an alarm). The bypass time period is determined individually for each partition.
 9. **Access to cash dispenser** – code which activates the function of access to a cash machine.
 10. **Guard** – global code, which may be used for making rounds by guards in all system partitions. Using of this code (typing [CODE][#]) on a LCD keypad or a partition keypad at the partition to which a specific user doesn't have access, generates a “Guard Round” event and activates the partition bypass. Using of this code on the code lock keypad or getting access by means of a proximity card or DALLAS chip generates the event of the “User Access” type. The settings of access control module options decide whether the events mentioned above are generated or not. When the guard is provided with access to partitions, the partitions may be controlled in a way similar to the control of the “normal” type code. Using the guard's code, card or DALLAS chip at the equipment assigned to the partition (also in the LCD keypad), where the guard round is programmed, starts the time countdown to the next guard round from the beginning.
 11. **Schematic** – code providing the user access to the system by a time scheme. One of the eight time schemes as may be determined by the installer should be assigned to such a code. The access scheme is based on 64 system timers. The user can control the system only when one of the particular scheme timers is active. Also, duration of the actual code must be set (0-254 days) – entering 0 will set an indefinite duration (until cancelled).
- **Rights** – this indicates which functions are accessible to the user. The user addition function suggests the list of rights limited to the rights of the user who enters a new user (the user who enters a new one cannot provide a new user with access to functions which he cannot call by himself).

Note: *It is possible to create in the service mode a „template (mask) of basic rights” assigned to each new user (or administrator). Additional authority, not indicated in the template, may be individually granted to the user (or administrator). This reduces the time of entering a large number of new users into the system. Such a template will be created by the installer by means of the function called „Active rights” (→ Service mode→ Options→ Active rights).*

- **Name** – user name, which appears in selection lists, printouts and when viewing the events memory.
- **Existence time** – parameter, which is programmed for codes with defined validity period only (see Type = 3, 4 and 11).

After the new user is added, the control panel indicates the number of the user in the system, which is sent to the station in events that contain this number together with the code (when monitoring in Ademco Contact ID format is activated).

4.6 PREFIXES

Control of the system may require entering additional digits called a **prefix** (service settings) directly before the access code. The prefix length (1 to 8 digits) is determined by the installer with the service function: →Options; →Prefix length (only from LCD keypad). There are two kinds of prefixes:

- Normal** – the prefix normally entered before each use of the code, by default programmed as 0 or 00, or 000 ... (the number of zeros depends on the length of prefix).
- Duress** – the prefix normally entered before use of the code in emergency, e.g. when the user is forced by third parties to disarm the system, bypass the zones, etc., by default programmed as 4 or 44, or 444 ... (the number of fours depends on the length of prefix). Using this prefix before the code results in the **duress** alarm code being sent to the monitoring station and activation of the DURESS ALARM output.

For security reasons, it is useful to periodically change the prefixes. The Administrator of the object is authorized to change the prefixes and define the change *Recall time* (see function →Change prefix).

Using the installer code does not require knowledge of the prefix - entering any digits instead of the prefix will do. It is important that the number of entered digits correspond to the length of prefix.

Note! Changing the length of a prefix restores its default value.

4.7 MONITORING

The CA-64 control panel phone communicator may report events to two stations. Each station has two telephone numbers assigned (one basic and one backup), and has the possibility of determining different transmission formats. When reporting to one station, the control panel makes consecutive attempts to dial alternately the basic and backup numbers.

When the “Station 1 or Station 2” mode is on, the control panel makes consecutive dial attempts in the following sequence: station 1 basic number, station 1 backup number, station 2 basic number, station 2 backup number, station 1 basic number and so on, until the number of attempts preset for each station is reached. After the programmed number of attempts is completed, the control panel suspends monitoring either until a next event occurs or for the time defined by the service (after that time elapses, the control panel starts the next series of attempts to transmit the message).

Note: 8 is the typical value for the “Repetitions” parameter, and 30- for the “Suspend time” parameter (occurrence of a new event resumes sending all the events not yet transmitted).

Events in the system are divided into eight classes:

1. alarms from zones and tampers,
2. alarms occurring in partitions (e.g. PANIC, fire alarm from the LCD keypad),
3. arming and disarming,

4. zone bypass,
5. access control,
6. system troubles,
7. functions used,
8. other events in the system (e.g. start of the service mode).

Event of 5 and 7 classes are not monitored. Other events are transmitted depending on transmission format selected.

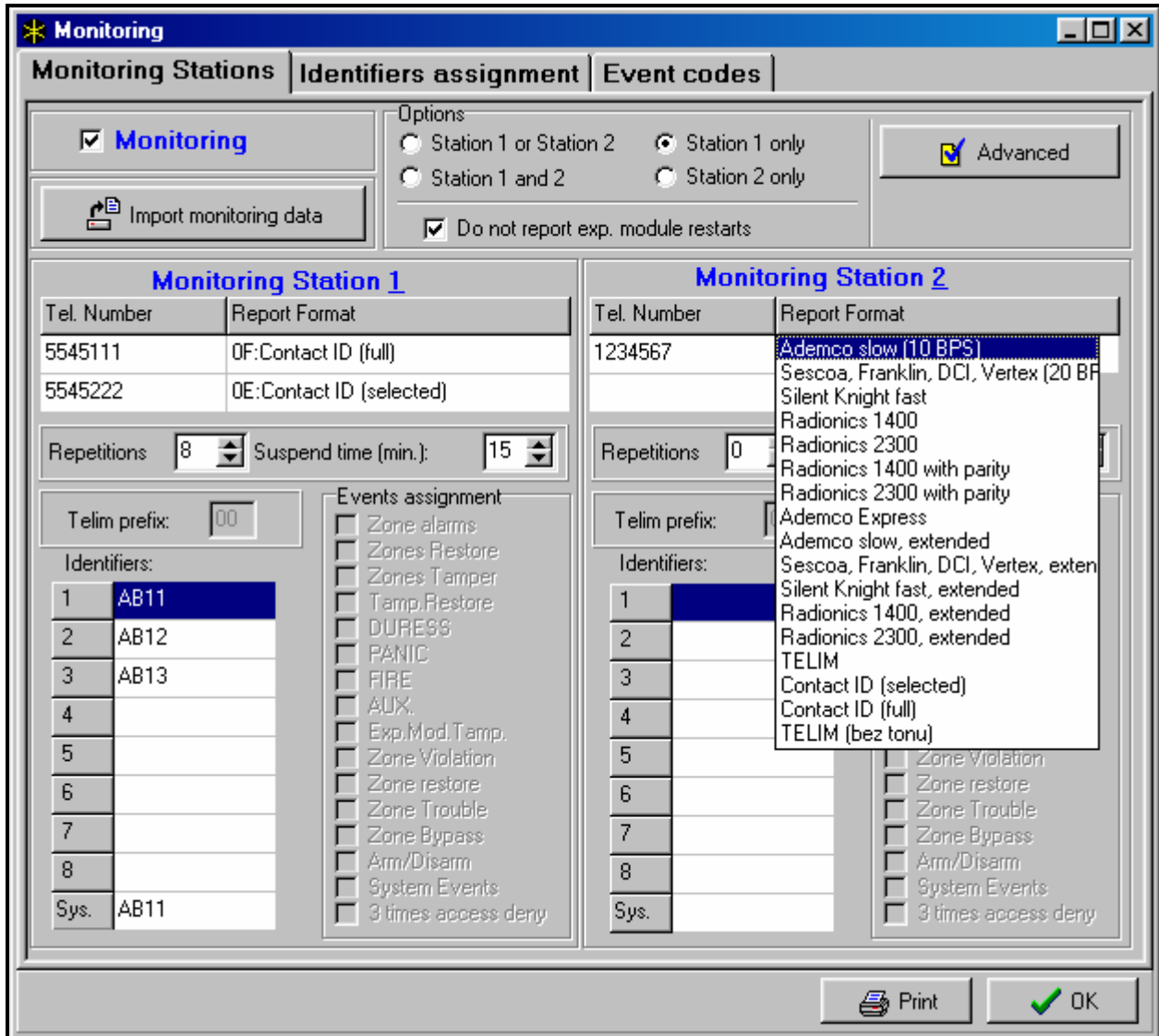


Fig. 8. Window for format selection and definition of identifiers.

- For pulse formats and Ademco Express it is necessary to program event codes. Only those events are transmitted which are assigned to a valid identifier (i.e. those which have at least three characters different from "0") and whose code is different from "00".
- When the "E: Ademco Contact ID (selected codes)" format is selected, the events are sent which would have been transmitted in pulse formats, the programmed code being of no relevance, since the control panel transmits codes according to the format specification.
- When the "F: Ademco Contact ID (all codes)" format is selected, there is no need for the installer to program any event codes and/or assign events to identifiers. The control panel transmits codes according to the format specification and the defined division into objects.

Notes:

- When the „E: Ademco Contact ID (selected codes)” format is selected, the control panel will only transmit the events which can be transmitted in pulse formats. Not all possible events have their equivalents in pulse formats. Programming of codes for all possible events in the system would require dozens of identifiers to be reserved for the control panel.
- For the E and F (Ademco Contact ID ...) formats, each object has its own identifier. Therefore, the identifiers of non-existing objects need not to be programmed. In the system event identifier field (events of class 6 and 8), you should re-enter the identifier of the object which “is responsible” for the system (for example, the object, where the control panel is installed).
- For the E format, the assignment of partitions, zones, keypads and expanders to identifiers does not need to reflect the division of the system into objects. But it is essential that a value different from “0” be programmed. The control panel transmits all events in the object with a single identifier according to division of system components among the objects.
- For the operating mode “Station 1 or Station 2” (and “Station N only”, with dialing both numbers), it is not possible to select the F format for just one number and another format for the remaining numbers, because it may occur that the event transmitted in format F cannot be converted into the type 4/2 code.

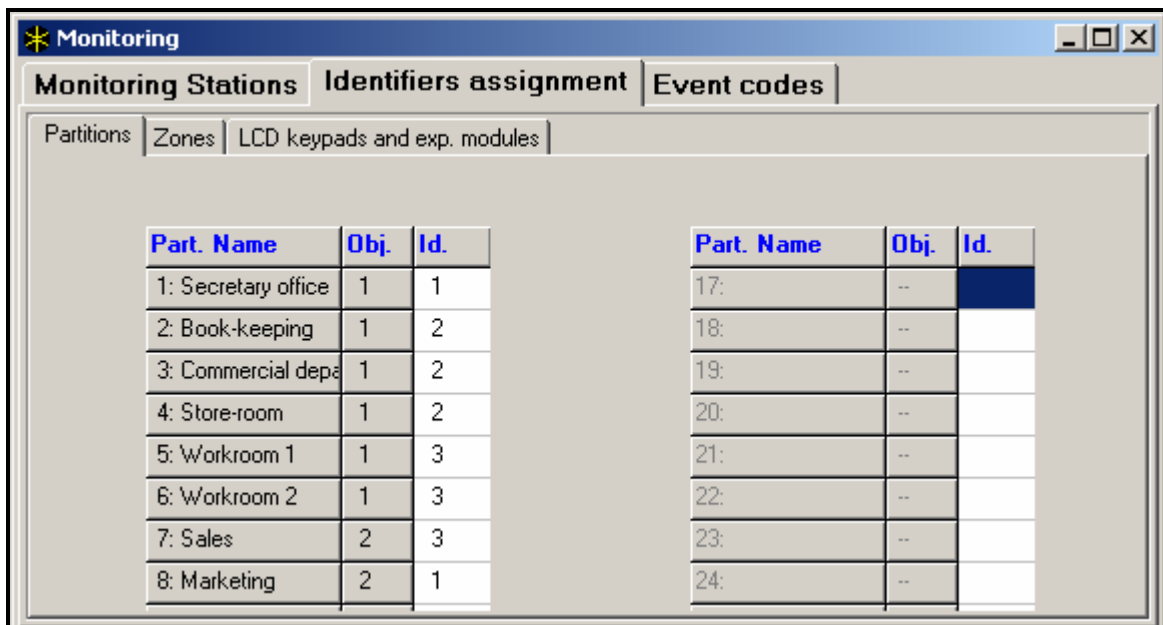


Fig. 9. Window for assigning partition events to identifiers.

For the pulse formats, individual events are assigned to identifiers. This allows optimum utilization of the available space for codes (8 x 225 codes = 1800 codes) – events from smaller objects may be grouped with a single identifier, and several identifiers may be assigned for larger objects.

Event codes are programmed after the division is made. The DLOAD64 program (and corresponding service functions) shows all events assigned to the identifier, which facilitates correct programming of codes (the event code window shows only the fields for those codes which will be transmitted with the given identifier – see Figure 10).

System events and troubles are transmitted with their own identifier. Figure 11 shows the events assigned to this identifier.

Notes:

- The “Settings reset” event is caused by the service functions, which restore the factory settings of the system. The number transmitted in the Ademco Contact ID format inform, which settings are reset (0 – control panel settings reset, 1 – reset of codes). Clearing of the event memory is transmitted with a separate code.
- The “RAM memory error” event informs of error(s) in the settings memory that is backed-up with a 3.6V battery. If the settings are stored in the FLASH memory, detection of this error forces “Module restart” that will be followed by “Settings restore”.
- “Module Restart” appears at each power supply connection.
- The CA-64 control panel allows a monitoring test of two types: transmitting the “Periodical test of monitoring” event either every day at a specified time or after a programmed time period from the last communication with the station (it is possible to activate the both types simultaneously). An additional transmission may be initiated with the user function, provided the “Manual transmission test” code is programmed.
- Checking communication with the station is facilitated with the “Station XX test” function (in the “Tests” menu of the user functions), accessible after station phone numbers, system event identifier and “Monitoring test” code have been programmed. Calling of this function initiates monitoring, when the control panel informs about the current transmission phase and the test result at the keypad.
- The event codes shown in Figures 10 and 11 are taken at random just to illustrate an example of programming. They should be programmed according to the recommendations of the monitoring station maintenance staff.

The screenshot shows a software window titled 'Monitoring' with three tabs: 'Monitoring Stations', 'Identifiers assignment', and 'Event codes'. The 'Event codes' tab is active, displaying three tables for programming codes.

Zone No:	1	2	3						
Alarm (zone)	11	11	11						
Zone restore	21	21	21						
Zone tampering	31	31	31						
Tamper restore	41	41	41						
Zone trouble	51	51	51						
Trouble restore	61	61	61						
Zone Bypass	71	71	71						
End of Zone Bypass	81	81	81						
Zone violation									

Part.:	1	2	3	4	5	6	8	10	11
Arming	12	12	12	12	95	96	98	9A	9B
Disarming	22	22	22	22	A5	A6	A8	AA	AB
Alarm clearing	32	32	32	32					
Alarm DURESS	42	42	42	42					
Auto arming suspend	52	52	52	52					

Kpd./Exp. Module:	K:00	K:02	E1:2	E1:3	E2:0	E2:1	E2:2	E2:3
PANIC alarm	12		13	13				
FIRE alarm	13		23	23				
AUX. alarm	14		33	33				
Tampering	15	15	15	15	15	15	15	15
Tamper restore	16	16	16	16	16	16	16	16
Alarm - unauthorized acc			17	17	17			
3 wrong access codes	18	73	18	18	73	73	73	73

Fig. 10. Programming of monitoring codes for pulse formats.

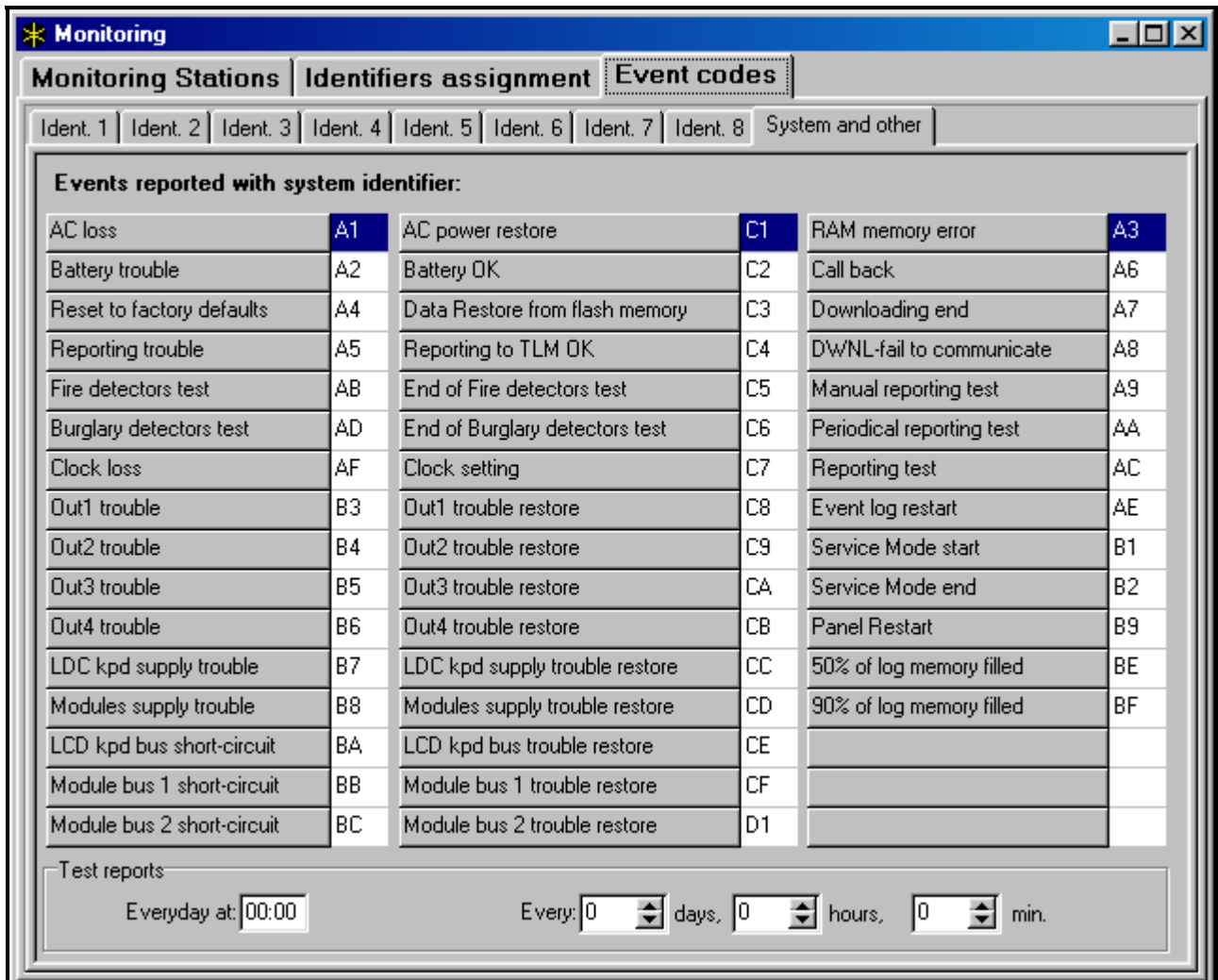


Fig. 11. System event codes.

4.8 MESSAGING

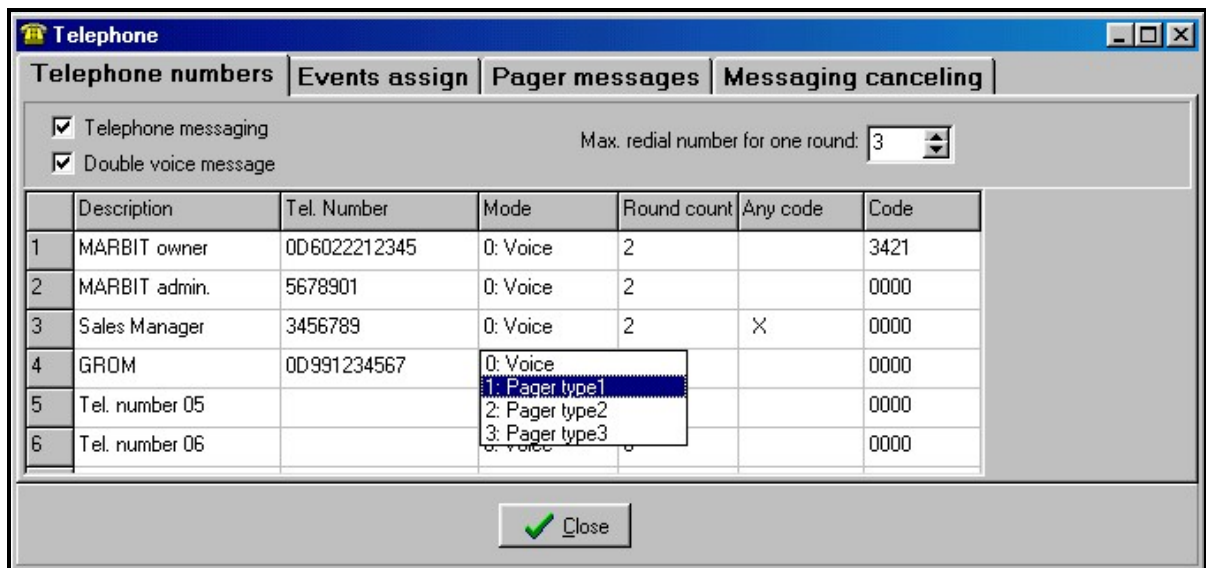


Fig. 12. Programming of a phone number for messaging.

The messaging function embedded in the control panel CA-64 allows notification of alarms with messages sent from voice synthesizers or transmitted to pagers. Messaging is performed independently from monitoring but monitoring has the priority. If in the course of

messaging some events occur which must be reported to the monitoring station by the control panel, monitoring will be included in between the messages sent.

Messages may be transmitted to 16 phone numbers. It is possible to send 16 different voice messages and 64 different pager messages.

During voice messaging, it is possible to acknowledge the message receipt. A special code connected with a telephone number is used for this purpose (it is possible to set any code – four digits transmitted with DTMF mean receipt of a message). The control panel acknowledges the code receipt with a special signal. If there is a number of messages to transmit to a single phone number, all these messages are transmitted during a single connection. In this case, the signal confirming that the message is received is different (handshaking that informs that further messages are awaited).

Since it is possible to define in detail how each alarm is to be communicated, the CA-64 control panel allows to organize an additional monitoring, based on the messaging function, that operates simultaneously with the basic monitoring. The way of defining the rules of communicating the alarms for zones is shown in Figure 13. The rules of communicating the other alarms are programmed in the same way. The messaging may also include information on power supply trouble.

Note: When communicating an alarm, the control panel performs a cycle of phone calls dialing all specific phone numbers in sequence. The numbers which confirmed alarm message receipt with a code are not dialed any more. Other phone numbers are informed in the next cycle according to the defined number of repetitions.

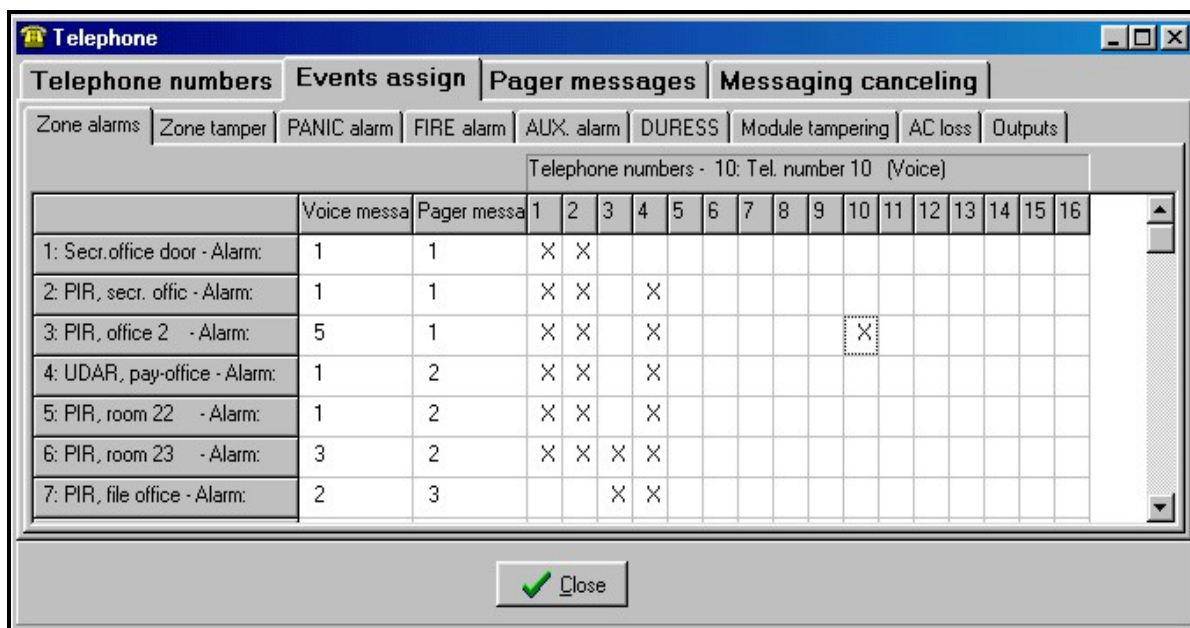


Fig. 13. Defining the way of communicating alarms for zones.

In order to activate the messaging function you should:

1. Select the „*Telephone messaging*” option and set the maximum number of redials in one queue (from 1 to 7) if the number is busy.
2. If, after voice connection is established, the message is to be repeated twice, select the „*Double voice message*” option.
3. Program the telephone numbers to be notified, and set the following for each number:
 - description (up to 16 characters)
 - messaging mode (voice, pager)
 - round count (how many times the control panel will dial the given number - from 1 to 15)
 - by default, zero is set, which means no telephone messaging

- how the notification receipt is confirmed – select the „Any code” option or enter the confirmation code (to cancel subsequent dialing of the given number).
4. Set the following parameters for corresponding events which will initiate messaging:
 - number of voice message synthesizer (from 0 to 15)
 - number of pager message for test messaging (from 1 to 64)
 - numbers of telephones to which the messages will be sent.
 5. Select partitions for each telephone number, from which the user will be able to cancel messaging.
 6. According to the circumstances, set the „Messaging canceling” option to enable the telephone messaging to be canceled together with alarm canceling.

4.9 ANSWERING A PHONE CALL

The control panel CA-64 is provided with the function of answering external phone calls. Only the users, who are assigned with a special “**telephone code**” (see: *Codes and users*) may have access to this function. The panel can answer the calls in one of two modes:

- **single calling mode** - the panel answers the call after a specified number of rings (if the code be incorrect, the control panel will not answer any incoming calls for 4 minutes);
- **double calling mode** – having dialed the control panel number, wait for the specified number of rings, then hang up and (within 3 minutes) redial the control panel number. After the redialing, the control panel should immediately answer the call.

For detailed information on answering the phone calls see the USER MANUAL.

4.9.1 CONTROL VIA TELEPHONE

The function of phone call answering allows also the control of REMOTE SWITCH type outputs (see: USER MANUAL).

In order to start the CONTROL VIA TELEPHONE function do the following:

1. Select the options: „Answering” and „Remote control”.

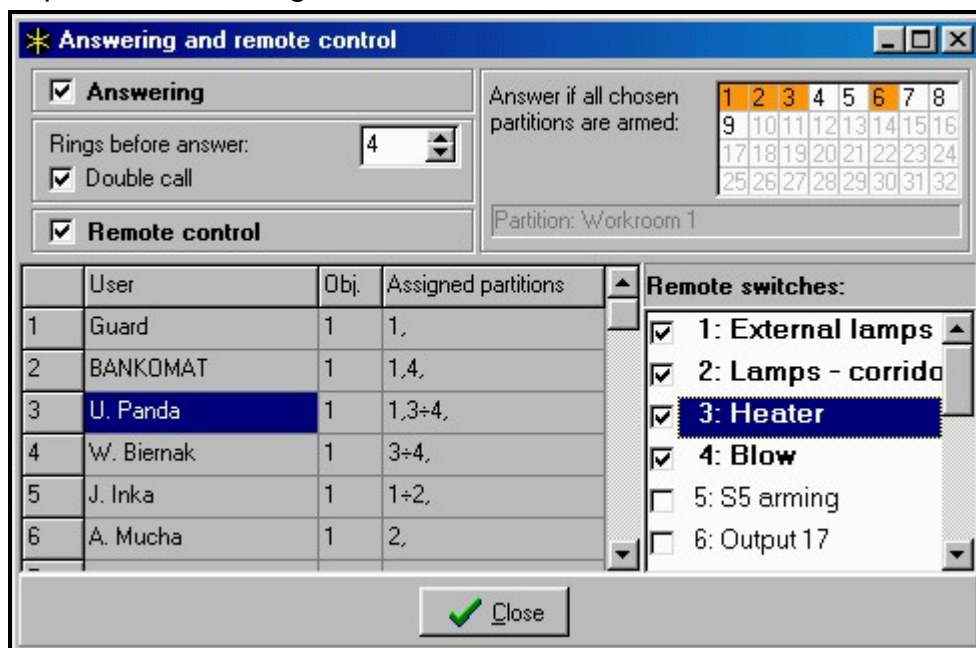


Fig. 14. Defining the remote switches which may be controlled by the user.

2. Define how the connection to the control panel will be established:
 - double call (if this option is not selected, the control panel will answer the call after the telephone number is first dialed),

- rings before answer.
- 3. Select the partitions which must be armed so that the control is available (with a possibility to restrict access to the control).
- 4. Program telephone access codes for the users who will perform the control function (user editing).
- 5. Program suitable outputs as the REMOTE SWITCH type.
- 6. Assign the REMOTE SWITCH outputs to the users so that they can effect the control.

Note: *Not all cellular telephones allow DTMF control.*

4.10 CONTROL OF OUTPUTS FROM LCD KEYPAD

The control panel makes it possible to control from the LCD keypad the following types of outputs: MONO SWITCH, BI SWITCH and REMOTE SWITCH (see: USER MANUAL).

To start the control function you should:

1. Program the parameters of control outputs (type, cut-off time, polarization).
2. Select how the output status will be indicated (standard or selected zone status).
3. Connect suitable devices to the outputs, and supply suitable signals to the zones indicating the equipment status.
4. Assign control outputs to the groups (4 groups can be created) and to the partitions from which triggering will be possible (telephone relays are not assigned to partitions).
5. Grant the CONTROL authority to the users who are to have access to this function, and assign partitions to trigger the controlling outputs.

4.11 REMOTE CONTROL

Two programs, DLOAD64 for use by the service (installer) and GUARD64 for use by the user, allow the CA-64 control panel programming and control. Both programs run in Windows9x/ME/2000/XP environment.

The DLOAD64 program enables data exchange between the computer and the control panel, and ensures convenient monitoring of the status of zones, partitions, outputs, module tampers, panel controlled doors, etc. For the purpose of programming, communication between the computer and the control panel can be established in several ways:

- direct connection via the RS-232 port of the alarm control panel mainboard,
- by means of telephone line via the control panel internal modem (this programming method makes available all the downloading functions, but as the transmission rate is limited to 300 bauds, it takes longer to perform the functions),
- by means of telephone line via an external modem connected to the RS-232 port on the control panel mainboard,
- through the GSM-4 communication module, used as an external modem (connected to the RS-232 port of the control panel mainboard), connecting to the computer via the GSM mobile telephone network.

Note: *The data transmission service (HSCSD/CSD - modem transmission) is usually available as part of the basic service pack offered by the cellular network operator, however before running the program it is advisable to make sure that you can use the network.*

The GUARD64 program provides visualization of the protected facility on the computer monitor, operating the system from an independent on-screen LCD keypad, access to the event log, as well as creating and editing the system users. For the purpose of programming,

communication between the computer and the control panel can be established in a number of ways:

- direct connection through the RS-232 port of LCD keypad - this operating mode can be used simultaneously on all connected LCD keypads,
- LAN/WAN network (TCP/IP communication) by means of the *G64_server* program running on the computer connected to the RS-232 port of LCD keypad,
- by means of telephone line via an external modem connected to the RS-232 port on the control panel mainboard,
- through the GSM-4 communication module, used as an external modem (connected to the RS-232 port of the control panel mainboard), connecting to the computer via the GSM mobile telephone network.

4.12 CONTROL PANEL STARTER

The control panel software is stored in the FLASH memory to allow programming on site (without removing the memory chip from the control panel mainboard). The software consists of two parts: the STARTER program designed for programming the FLASH memory, and the control panel program. When the STARTER program is in use, the control panel normal functions are deactivated (status of electronic circuit protectors only is monitored).

Operating status of the STARTER program is signaled by rapid blinking of the LED at the telephone line relay, corresponding message on all LCD keypads, and blinking of the LEDs in keypads / partition keypads.

The programming mode of the STARTER program may be entered in two ways:

1. By calling it from the service mode function menu.
2. By switching on the control panel power supply with RESET pins shorted. Remove jumper immediately after the control panel has switched on power supply at outputs supplying keypads and expanders (when the jumper is not removed before calling the control panel program by STARTER, downloading via RS-232 will be started or the control panel will enter the service mode).

Notes:

- *When the STARTER program is in the programming mode, the “STARTER 3.1 is running...” message is displayed at LCD keypads. This signals readiness to operate with the FLASH64 program (it should be started in the computer connected to the control panel mainboard via RS-232). If the STARTER program receives no command from the computer within 2 minutes, the control panel program will be restarted.*
- *When the control panel is connected to the computer, the STARTER program may be stopped by calling the “Restart CA-64” command in the FLASH64 program (Ctrl-F2, then indicate the port, to which the control panel is connected).*

5. CONTROL PANEL INSTALLATION

The control panel PCB contains electronic components sensitive to electric charges. Prior to installation, these charges must be removed. During installation, avoid touching any elements on the control panel PCB.

The CA-64 control panel should be installed indoor, in spaces with normal air humidity. Permanent (not disconnectable) 230 VAC power supply with protective ground should be available in the room. The telephone line must be made with the use of four-wire cable to make possible connection of the control panel to other equipment (telephone, fax, etc.).



Notes:

- *Install PCB fixing pins prior to the control panel housing installation.*
- *When installing the housing, be careful not to damage cables which will pass through openings in control panel housing rear panel.*
- *Switch off mains power supply and battery power supply when connecting LCD keypads and other components powered from control panel outputs.*

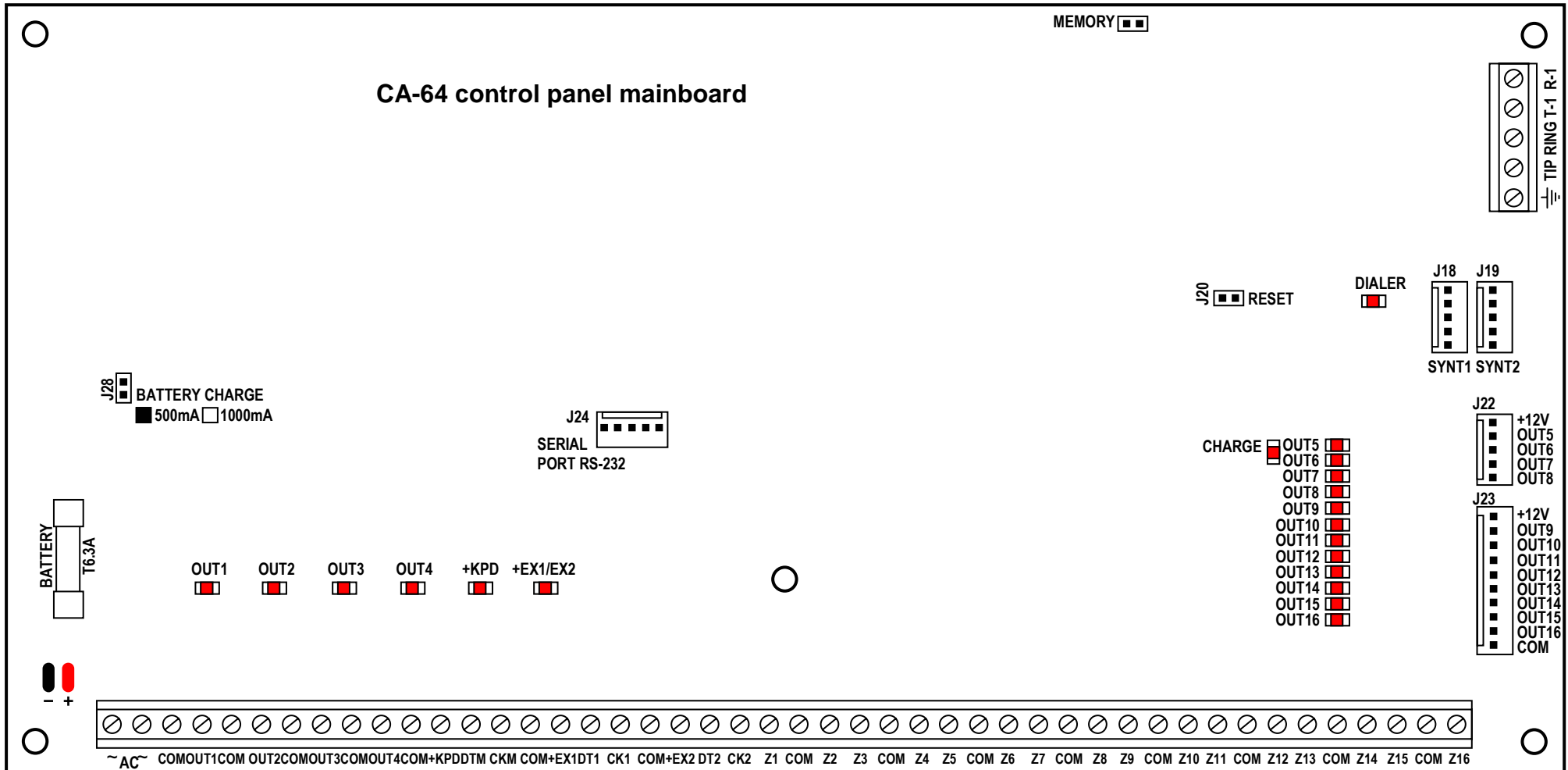
CAUTION!

Since the control panel is powered from 230VAC mains, carelessness when wiring or incorrect wiring may lead to electric shock and pose danger to life!

Be very careful when making connections of the control panel. The power supply cable cannot be live when installing and connecting it to the control panel!

CA-64 control panel mainboard

MEMORY



Board terminals:

- AC** - module power supply inputs (20...24V AC)
- Z1 to Z16** - zones
- OUT1 to OUT16** - programmable outputs
- +KPD, DTM, CKM** - keypad bus
- +EX1, DT1, CK1** - first bus of expanders
- +EX2, DT2, CK2** - second bus of expanders
- COM** - common

**T-1, R-1
TIP, RING**

**+12V
SYNT1, SYNT2
RS-232**

- extension telephone line (telephone set connection)
- outside telephone line
- protective terminal - ground (connect to protective circuit only)
- supply output
- connectors for voice synthesizers
- connector for printer or service computer

5.1 CONNECTION OF POWER SUPPLY


The control panel is permanently connected to a main power source. Hence, before making the connections familiarize with the electric system in the facility. For powering the control panel choose the circuit which is always live. The power supply circuit should be protected with a proper fuse.


CAUTION!

Before connecting the control panel make sure that voltage is off in the power supply circuit to which the control panel is to be connected.

5.1.1 DESCRIPTION OF ELECTRIC CONNECTIONS

The AC power supply unit encased in the plastic box is fully electrically isolated from the metal housing.

- Connect the 230V alternating voltage leads to the transformer terminals marked "**AC 230V**".
- Connect the output voltage wires of the transformer secondary winding to the "**~AC**" terminals on the control panel mainboard.
- Connect the wire of the electric shock protection circuit to the terminal block provided next to the transformer and marked with the ground symbol . This circuit should also be connected to the control panel protective terminal.

The CA-64 mainboard allows an electric shock protection circuit (grounding) to be connected. The protective cable terminal is designated by the  symbol.



The „neutral” wire of the 230V AC mains supply must not be connected to it. If there is no separate electric shock protection circuit in the facility, this terminal must be left free.

Control panel power supply unit operates with input voltage of **20...24V AC**. The control panel is provided with the up-to-date pulse power supply unit, highly efficient and reliable, but, for its correct operation, it is necessary to ensure that input voltage at **maximum transformer load** by the control panel do not fall below **18V** (AC).

Attention should be paid so as not to cause overloading of the control panel power supply in the security system. It is advisable to make a **load balance** for the power supply. The total current inputs for the consumers (detectors, keypads) and the battery charging current may not exceed the power supply capacity. In case of a higher electric power demand, an additional power supply can be used for some of the security system consumers (e.g.: APS -15, APS-30 manufactured by SATEL). Table 1 (at the end of this manual) shows an example of estimated balance of current consumption by the system, and an example of battery selection.

Stabilized voltage of the control panel power supply is factory set at 13.6 – 13.8V and should not be changed.

5.1.2 CONTROL PANEL POWER SUPPLY STARTING PROCEDURE:

1. Connect the backup power supply wires to corresponding battery terminals (red to battery plus, black to battery minus). **The control panel will not start after connecting battery alone** (without mains power supply) but it will operate in case of 230VAC failure when it was started earlier.

Note: *When the control panel is working and the battery supply voltage drops to approximately 11V, the control panel reports battery failure. After the voltage drops to approximately 9.5V, the control panel disconnects the battery (the system is stopped).*

2. Connect the 230 VAC mains – the control panel starts to operate.

The specified here sequence of power supply switching on (first battery, then 230VAC mains) ensures correct operation of power supply unit and control panel electronic protections, which allows to avoid troubles of alarm system components due to installation errors. Start the modules with their own power supplies in the similar way.

CAUTION! *In situation, when total disconnection of control panel power supply (mains and battery) is necessary, switch on the control panel in the way described above (first battery, then mains 230 VAC).*

After all wiring is made and installation correctness is confirmed, you may start the system. It is recommended to start operation with the control panel without signaling devices. The signaling devices may be connected after completion of parameter programming for the alarm system.

For systems with extension modules with their own power supply, it is recommended to start the control panel first, then other system components in sequence.

CAUTION !

Since the control panel is not provided with main switch to disconnect mains, it is important to instruct the alarm system owner or user on how to disconnect it from mains (e.g. by showing the fuse which protects the control panel power supply circuit).

5.2 CONNECTION OF LCD KEYPADS

Up to eight independent LCD keypads, designed for control and programming of the alarm system, may be connected to the control panel CA-64. When some keypads are being connected to the control panel, connect them in parallel. Since keypad bus data are addressed, all keypads operate independent of each other.

LCD keypads are to be connected to COM, +KPD, DTM and CKM terminals. The +KPD output makes it possible to power all eight keypads (this output is provided with electronic protective circuit breaker with a 3A limiter). Each keypad must be connected with its separate cable (it is recommended that a typical unscreened cable be used). Maximum distance between keypad and control panel is up to **300m**.

The lowest possible resistance of cables is important for correct operation of keypads. Depending on the distance between a keypad and the control panel the following number of cable wires must be provided for individual connections when using a cable DY 8x0,5 in:

Distance	Description	Number of cable wires
up to 100 m	Power supply +KPD and COM CKM and DTM signals	2 x 1 2 x 1
up to 200 m	Power supply +KPD and COM CKM and DTM signals	2 x 2 2 x 1
up to 300 m	Power supply +KPD and COM CKM and DTM signals	2 x 4 2 x 2

Notes:

- *CKM, DTM and COM wires must be in the same cable!*
- *Power supply measured at the LCD keypad terminal, when the backlighting is on, cannot be less than 11V.*
- *The presence of power supply voltage at the +KPD terminal is signaled by the fifth LED in the electronic circuit breakers block.*

- Keypads, which are installed far from the control panel, may be powered locally from an independent power source. These keypads are connected to the system with the use of CKM, DTM and COM signals.

TERMINALS DESCRIPTION	
KEYPAD	PANEL
KPD	+KPD
DTM	DTM
CKM	CKM
COM	COM
Z1 – to detector	Additional system zones
Z2 – to detector	

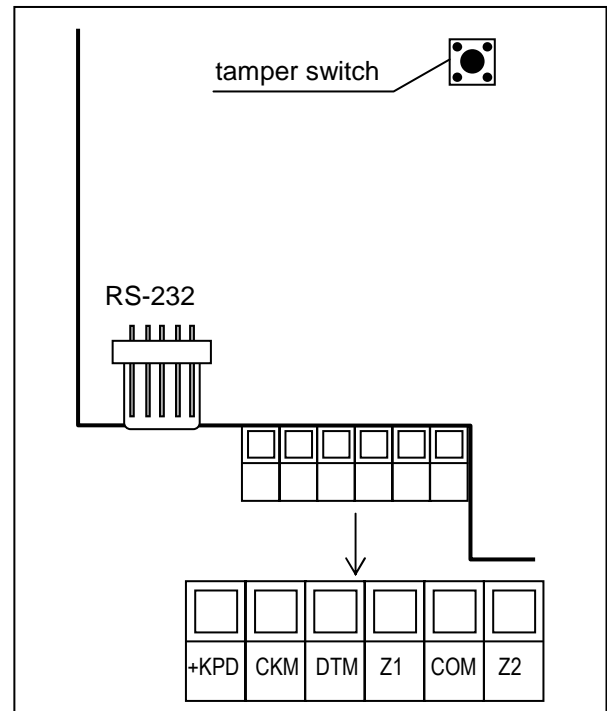


Fig. 16. CA-64K keypad PCB.

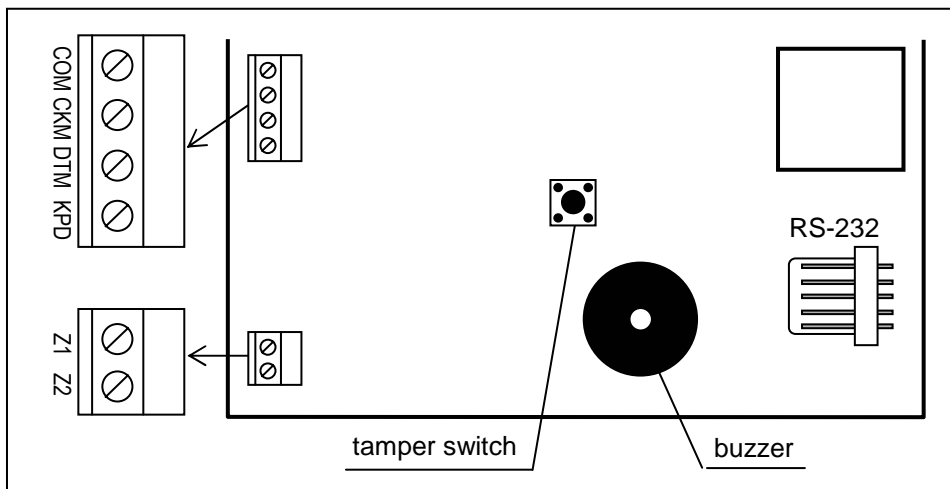


Fig. 17. CA-64KLCD-S keypad PCB.

Note: PCBs of the keypad types L and S differ from each other only in their external dimension and size of LCD.

The control panel identifies the keypads by their programmable addresses, which are saved in EEPROM (non-volatile memory). In the older versions of keypads, the address was set by means of jumpers on the keypad board.

The addresses must not be repeated ! The keypad address also indicates the numbers under which the keypad supervision zones Z1 and Z2 appear in the system. They are supported by the control panel in the same way as the mainboard zones.

Keypad address	Numbers of Z1, Z2 zones in security system
0	49 and 50
1	51 and 52
2	53 and 54
3	55 and 56
4	57 and 58
5	59 and 60
6	61 and 62
7	63 and 64

Note: If the system includes more than 4 input expanders, the zone numbers of which coincide with the numbers of keypad zones, then, programming the keypad settings you must define whether the detector is connected to the zone of keypad or that of expander.

The keypad address can be programmed in two ways:

1. Directly (skipping the control panel service code):

- Turn off the keypad power supply and the data bus wires (CKM, DTM).
- Short the keypad terminals CKM and DTM.
- Turn on the keypad power supply.
- The following text will be displayed:

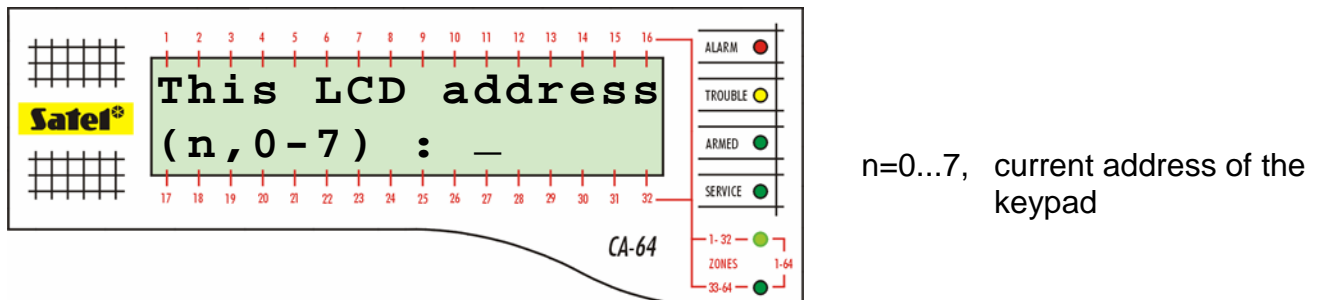


Fig. 18. Programming the keypad address

- Enter a new address within the 0-7 range. The keypad will confirm performance of the function with four short and one long beeps. The address can be changed again on pressing the [*] key.
 - Connect the keypad to the control panel as required (CKM, DTM).
2. By using the control panel service function:
- Activate the panel service mode (from any supported keypad): [SERVICE CODE][*], →Service mode.
 - Select in turn the items from the menu of displayed functions: →Structure; →Hardware; →Identification; →Keypad addr.
 - On the displays of all keypads a message will appear as shown in Figure 18.
 - Enter the appropriate address from the 0-7 range; the keypad will confirm performance of the function with four short and one long beeps; then, press the [*] key - the keypad will quit the address change function.

Notes:

- For the LCD keypads to be properly supported by the CA-64 control panel, the keypad identification function must be performed after setting the keypad addresses.

- *Setting the same address in several keypads will trigger the tamper alarm, and also will display the „This keypad is changed” message and disable operation of such keypads. To restore the operation of keypads, change their repeating addresses into unique ones. The changes can be made as described herein.*

The correctly connected keypad reports its restart and displays a date and clock or name, while incorrect wiring is signaled by displaying the message “No communication with control panel”.

System control is only possible after the **Identification of keypads** service function is performed. This function checks the addresses to which keypads are connected and registers them in the system. Disconnection of a keypad registered in the system causes tampering alarm. Any commands from a keypad not registered by the control panel are rejected (the message “Keypad is not serviced” appears on the keypad display).

The LCD keypad port RS-232 is designed for connection of a user’s computer. It operates with the Guard64 program that allows system control by means of a computer (virtual keypad, users authorization edition) and supervision (plan of the object showing statuses of partitions and detectors, viewing events memory).

Connection to the computer is permanent, made with the use of an ordinary unscreened cable. For a DY8x0,5 cable, the distance between the computer and the keypad can be up to 100 meters. Keypad connector signals are shown in Figure 19.

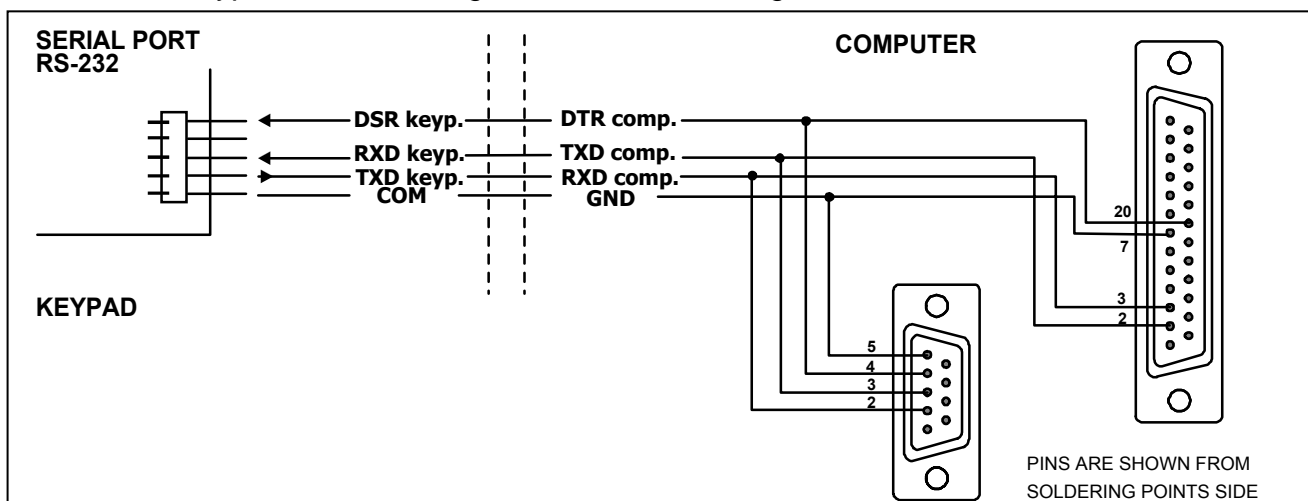


Fig. 19. Connection of the computer to the LCD keypad RS-232 port.

Note: *Switch on the “RS communication” option in parameters of keypads to which user’s personal computer is to be connected. Data exchange with the computer starts automatically when the Guard64 program is started.*

Each LCD keypad contains individual name and a set of parameters which determine its way of operation in the system. These are:

- **Partitions managed by keypad** – partitions, which can be armed/disarmed or alarm may be cancelled from the keypad. Control will be possible for those users, who have access to partitions specified here. When any partitions specified here is armed, the keypad LED *ARMED* blinks. When all partitions specified here are armed, this LED lights steadily.
- **Alarm indication** – list of partitions, for which a burglary alarm will be shown in the keypad. Alarm will be indicated by LED *ALARM* and message at the display will appear (when option “Alarm messages” – “partitions” is on). Additional option determines whether an alarm is signaled audibly.
- **CHIME signal** – list of zones, violation of which causes audible keypad alarm. This signal, as well as key sounds and exit time signaling can be automatically disabled after violation of the selected zone for a time period not exceeding 255s.

- **Quick Arm partitions** – partitions, arming of which will be activated after entering [0][#] on the keypad.

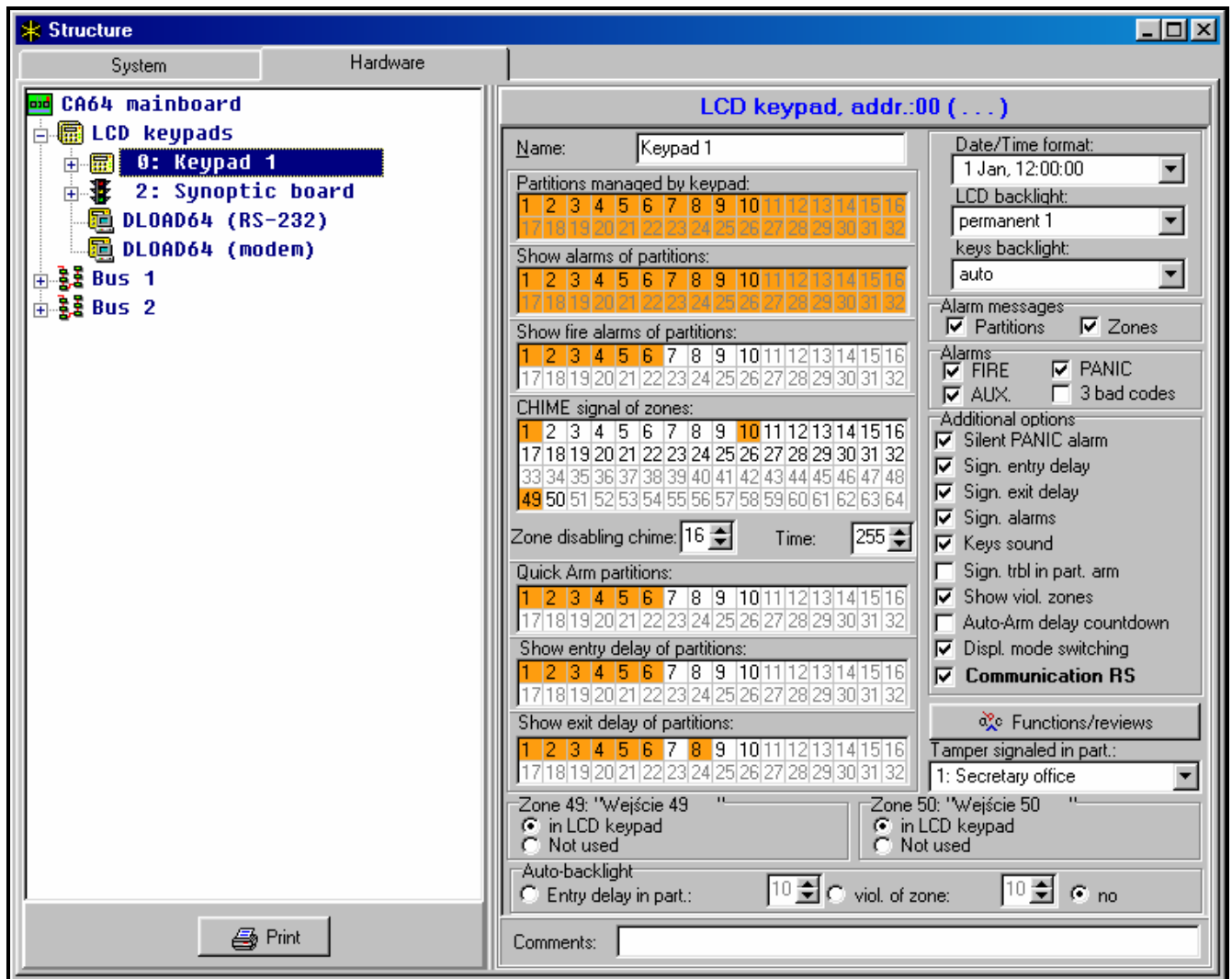


Fig.20. Parameter defining LCD keypad operation.

- **Time indication** – the keypad can display the entry/exit time counted down in the partitions served. Additional options make it possible to define whether the alarm will be signaled by sound.
- **Keypad zones** - each LCD keypad is provided with two zones which may be used in the security system. These are zones 49 and 50 for the keypad with address 0, and zones 51 and 52 for the keypad with address 1, and so on, up to zones 63 and 64 for the keypad with address 7. These zones can be also accessible in a zone expansion module, provided the maximum number of zone modules are connected. The options make it possible for each of the keypad zones to determine whether or not it will be utilized in the keypad.
- **Auto-backlight** – violation of the indicated zone or entry time countdown in the indicated partition may turn on the backlighting of keys and keypad display.
- **Date/Time format** - permits selecting the format of time and date display on the keypad
- **LCD Backlight** - selection of the display backlighting type.
- **Keys backlight** - selection of the keypad backlighting type.
- **Alarm messages** - the options define whether text messages on alarms in partition and zones are to be shown (the message contains name of partition/zone).

- **Alarms** – the options determine if the following alarms can be called from the given LCD keypad:
 - FIRE - fire alarm triggered by keeping depressed the [*] key,
 - AUX. – auxiliary alarm triggered by keeping depressed the [0] key,
 - PANIC – panic alarm triggered by keeping depressed the [#] key,
 - 3 wrong codes - alarm triggered by entering three wrong access codes.

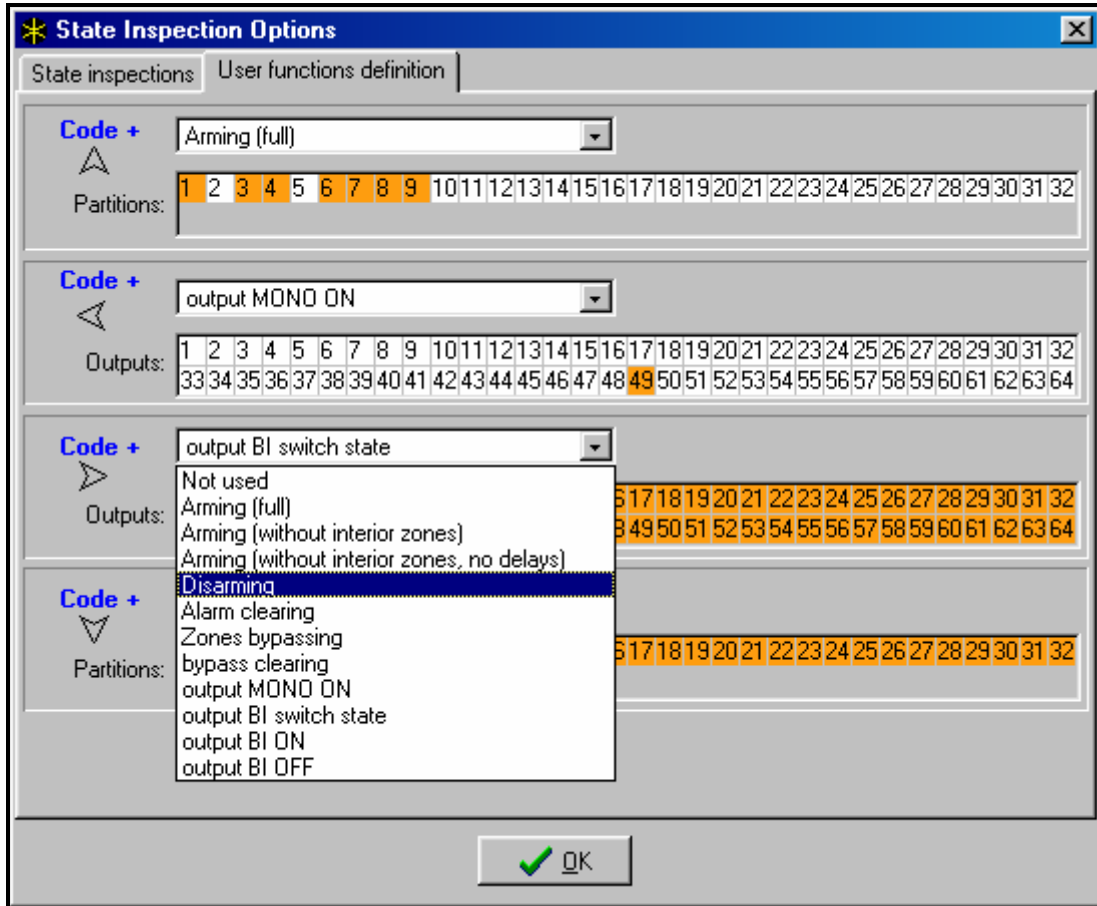


Fig. 21. Programming the arrow functions.

- **Additional options** – a set of additional options for activating some functions of the keypad:
 - *Silent PANIC alarm* - determines if the panic alarm called from the LCD keypad will be indicated as a silent alarm (with no signaling on alarm outputs) or as a normal, audible alarm
 - *Signaling entry delay* - determines whether the entry delay counting will be signaled by sound on the keypad
 - *Signaling exit delay* - determines whether the exit delay counting will be signaled by sound on the keypad
 - *Signaling alarms* - determines whether the LCD keypad will signal the alarm by sound
 - *Key sounds* - determines whether pressing the keypad keys will be confirmed by sounds
 - *Signaling troubles in partially arm* - determines whether the keypad will indicate system troubles (yellow LED) if some of the served partitions are armed (when all partitions are armed, troubles are not indicated)
 - *Show violated zones* – enabling the option means that the zones signaling CHIME in the keypad will be shown together with their name
 - *Auto-Arm delay countdown signaling* - activates audible signaling of the countdown to arming the partitions by timer (the signaling continues for the partition auto-arming delay time)

- *Display mode switching* – enabling the option makes it possible to switch over the display mode from system status to all-partition status by holding down the key "9"
- *Communication RS-232* - determines whether the keypad RS-232 port is enabled to interface with the Guard64 program - with this option enabled, it is possible to program the settings of the computer "virtual" keypad accessible from the Guard64 program
- **Functions/reviews** – options which make it possible to:
 - program the access to key functions („press and hold down" type) – for scrolling through system memory and status;
 - define the characters to signal the statuses of zones and partitions in the viewing functions;
 - select partitions the status of which will be permanently shown on the display;
 - assign the user functions to arrow keys (to be performed after entering the code and pressing the corresponding arrow).
- **Tamper signaled in partition** – defines the partition where alarm will be signaled after violation of the keypad tamper circuit and disconnection of the keypad from the system.

5.3 CONNECTION OF EXPANSION MODULES

The CA-64 control panel is provided with two buses designed for connecting the expansion modules (expanders). Both buses have the same priority and can be used in parallel (it is irrelevant which modules are connected to each bus). All modules are connected in parallel, and up to 32 modules may be connected to each bus.

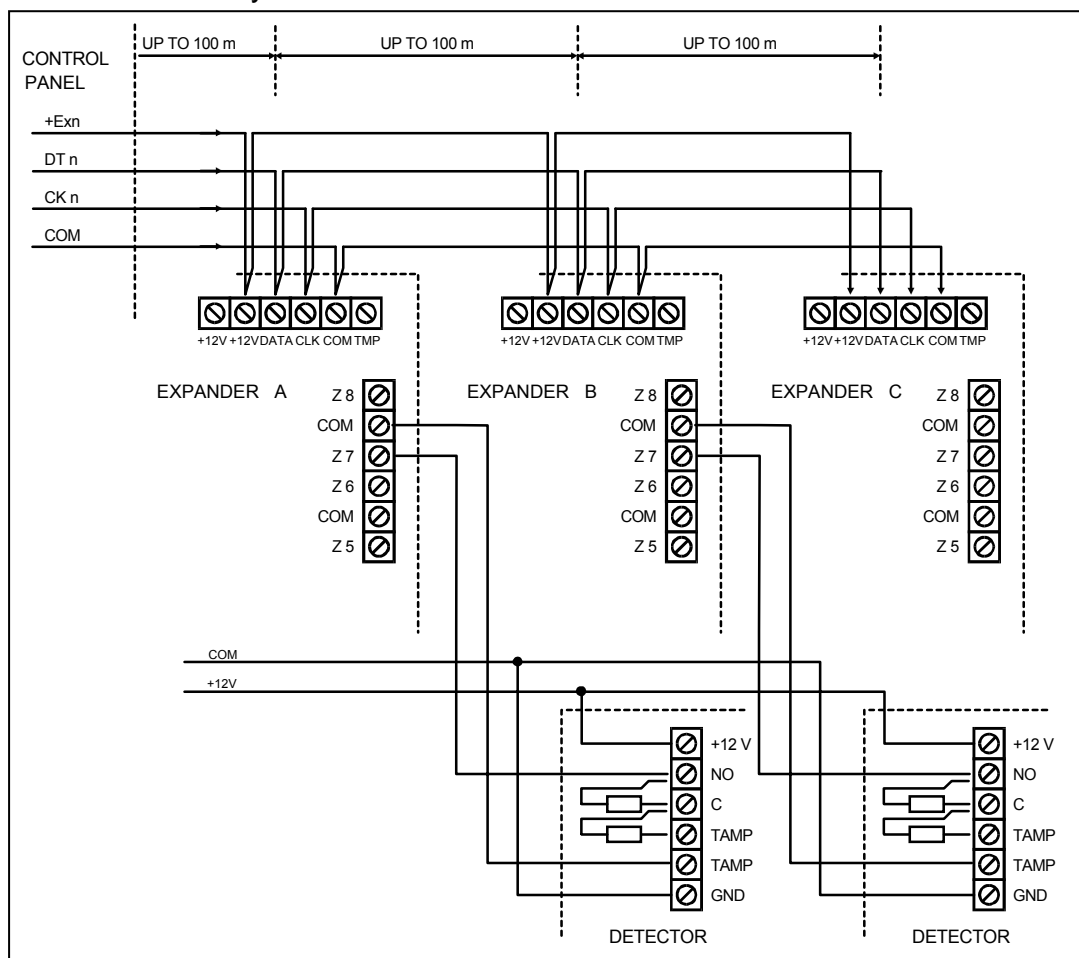


Fig. 22. Correct connection of modules for small distances between the control panel and modules, and way of detector connection.

Data transmission is carried out via DT1, CK1 and COM for the first bus, and via DT2, CK2 and COM for the second bus. Additionally, power supply for modules is provided at +EX1 and

+EX2 terminals. Both power supply outputs are connected to common electronic circuit breaker (limitation 3A), the presence of power supply voltage is signaled by the sixth LED in the electronic circuit breaker block.

The modules may be connected with the use of a typical unscreened cable used in alarm systems (for example, DY8x0,5). The DTn, CKn and COM signals should be supplied by one cable (not by separate cables). For small distances (up to 100 meters), when modules are only connected to the power supply cable, it is permissible to connect some modules one after one (see Fig. 22). Additional equipment connected to the power supply source must be supplied through separate cables (detectors connected to modules A and B).

Note: Connection of a fourth module after module C is not recommended when a DY8x0,5 cable is used. The module connected in this way may be not “seen” by the control panel. Resistance of cables at DTn and COM causes that logic level “0” at the control panel input may be higher than the maximum allowable level.

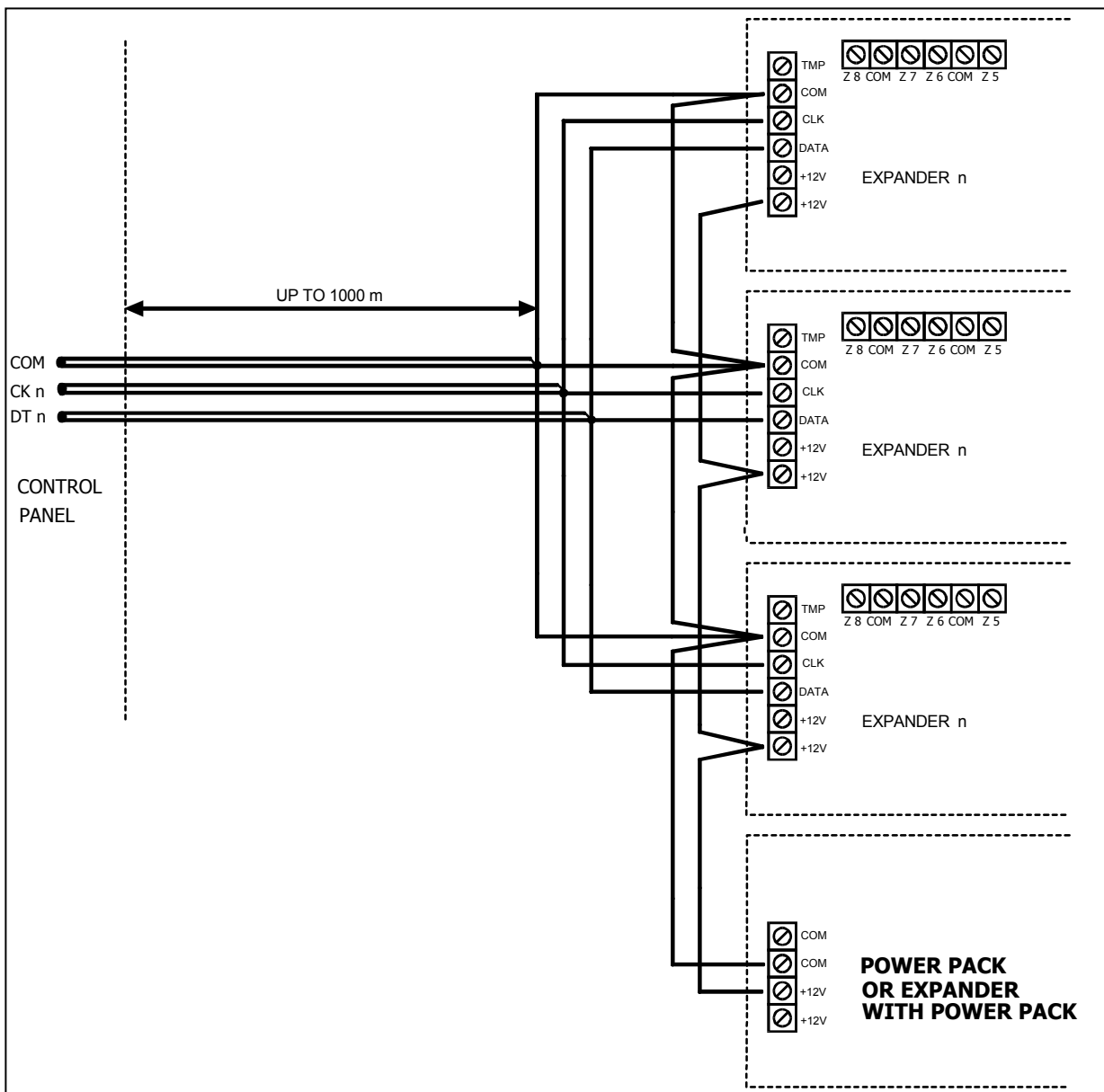


Fig. 18. Connection of module group located far from the control panel.

For large distances between the control panel and modules (up to 1000m), modules should not be powered from the control panel, and DTn, CKn and COM signals should use 2-wire cable. Additionally, the DTn, CKn and COM signals must be in one cable. It is possible to connect several modules in parallel and connect them to a single common cable through

which the DTn, CKn and COM signals will be connected (see Fig. 23). For example, when the distance from the control panel to the cabling node is 800m and the distance from the cabling node to the module is less than 100m, it is possible to connect up to 16 modules.

Each module connected to the bus should have its own, unique address. It is irrelevant which addresses are set for individual modules (the control panel receives information on module type and automatically sets optimum sequence of calling the modules for data). Address is set by means of switches marked *ADRES ABCDE*.

The control panel services the modules registered in the system by means of the **Identification of expanders** service mode function. This function determines expander addresses and types. Additionally, it sets a special random generated marker by which the module confirms its presence in the system. This marker is stored in module non-volatile EEPROM memory, and it may be changed in a next identification process only. For this reason, each module replacement, address change and change of module type under given address require running of the identification function again.

Notes:

- *The control panel does not service the modules when the identification function is not completed with message "Found xx exp. (xx new)".*
- *Wrong module connection can make impossible the correct identification of modules, which is signaled by the "Error! Two expanders have the same addr. !" message.*
- *Too high resistance of cables connecting the module to the control panel (large distance, too small number of wires for a single signal) may cause that the identification function does not see the module.*
- *When modules are served by the control panel, the LEDs at zone, output, synthesizer modules (and other, which are provided with operation signaling for service only) change their status.*

5.4 CONNECTION OF DETECTORS

CA-64 may operate with any detectors. Each control panel zone and zones of LCD keypads and zone modules may operate in the following configurations:

- **NC** (normally closed),
- **NO** (normally open),
- **EOL** (end of line resistor),
- **2EOL/NO** (NO type detector, double end of line resistor),
- **2EOL/NC** (NC type detector, double end of line resistor).

When a zone operates in a EOL configuration, use **2.2 kΩ** resistor to close the detector circuit. For 2EOL zones, detector circuit is closed with two resistors **1.1kΩ**. 2EOL type zones allow the control panel to control detector status and detector tamper switch simultaneously.

Any output with electronic protection (from OUT1 to OUT4) may be used to power detectors. This output should be programmed as POWER SUPPLY OUTPUT. For larger systems with additional power supply with high capacity batteries, detectors are powered from external power sources.

Figure 24 shows how to connect detectors to zones working in various configurations. Separation of the grounds of detector power supply and signal informing of the status of detector connected to the control panel monitoring zone, eliminates the influence of the resistance of wires on the detector status detection. Assuming that only one detector is connected to the cable and the cable is not very long, the installation may be simplified by leading a common single wire for power supply ground (COM) and signal ground (COM).

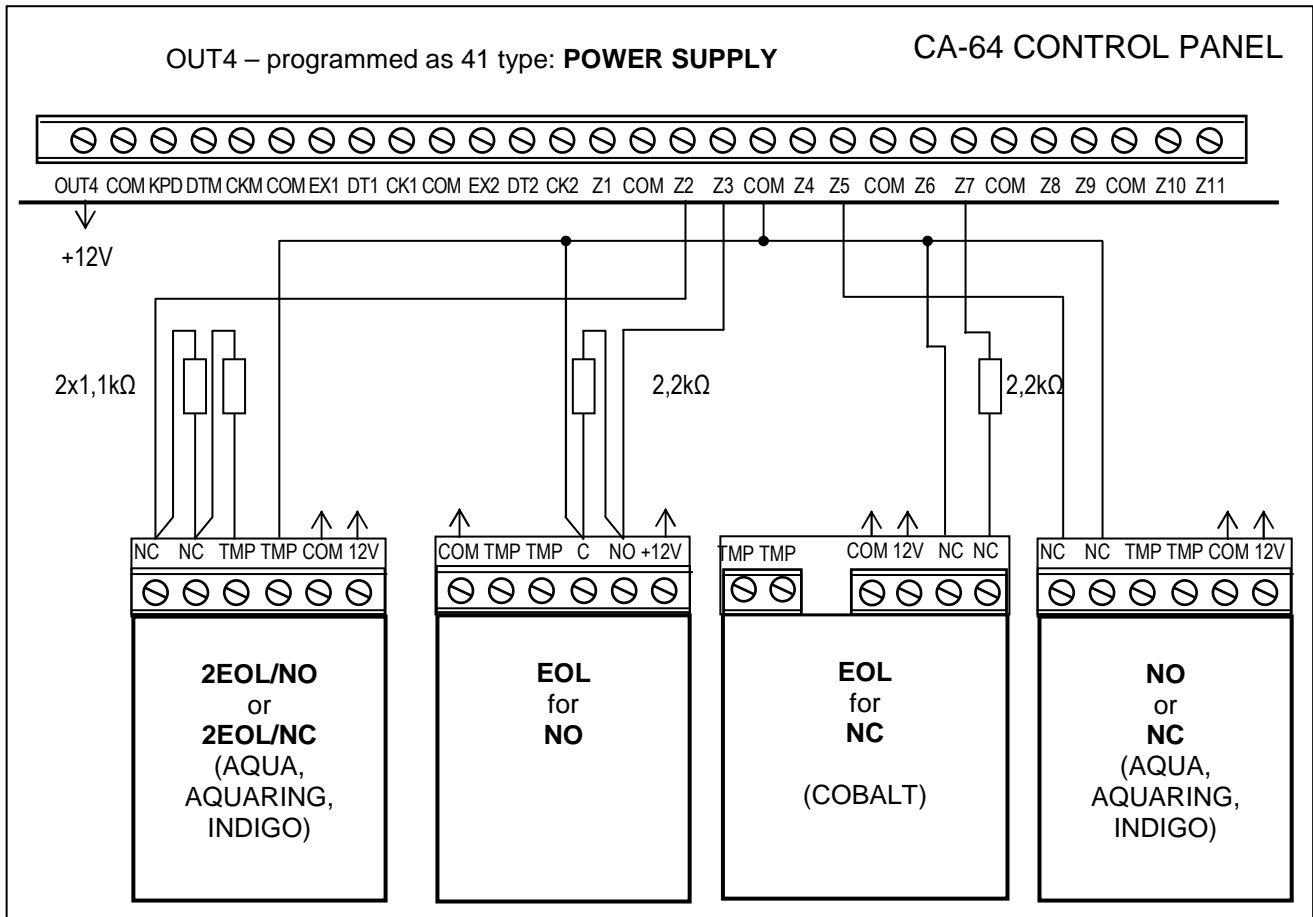


Fig. 24. Example of connecting 4 detectors in various configurations (with Z5 tamper circuit). NO and NC detectors in a 2EOL configuration are connected in the same way, it is only important to properly indicate to the control panel which detector is connected to the zone (2EOL/NO or 2EOL/NC).

Note: The recommended power supply circuit for detectors connected to expanders is shown in section „Connection of expansion modules”.

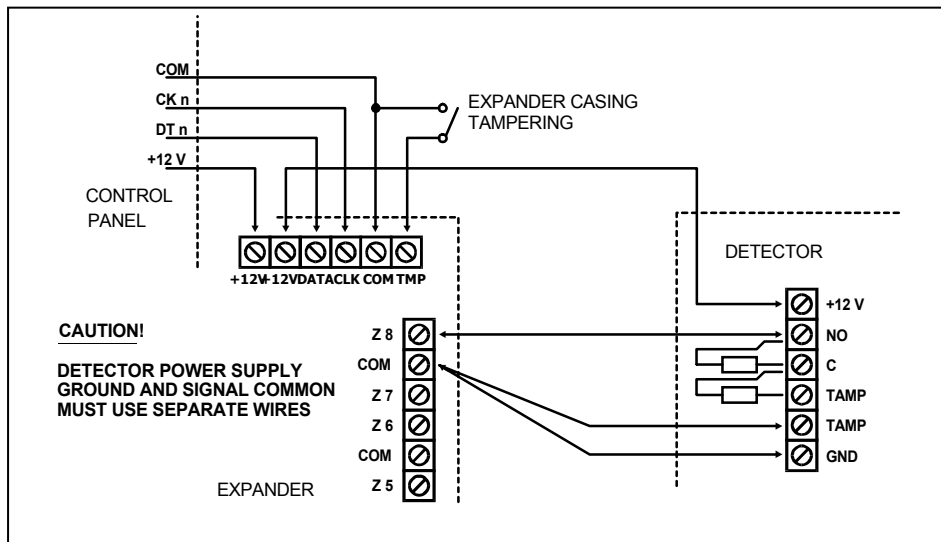


Fig. 25. Connection of 2EOL detector to the expander for small distance between the control panel and the expander (detector is located far from the expander).

5.5 CONNECTION OF SIGNALING DEVICES

The CA-64 control panel is provided with 16 outputs, whose application may be programmed. In order to connect a signaling device to the control panel, it is necessary to program this output as an alarm output.

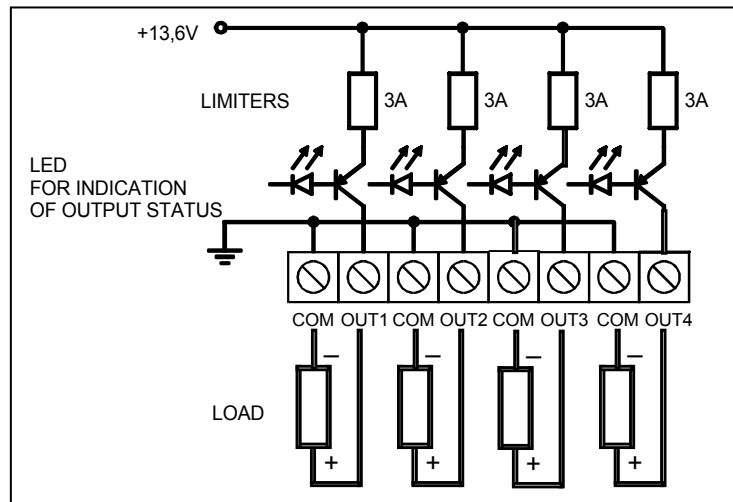


Fig. 26. Connection of a load (e.g. signaling device) to outputs OUT1..OUT4.

Four outputs are high-current with electronic circuit breaker set to 3A. Their structure and how the signaling devices without their own power supply (or without other loads) are connected to them are shown in Figure 26.

Notes:

- Outputs OUT1..OUT4 are provided with a load presence detection unit, which is active when output is not active. If a load is connected correctly and the control panel indicates the “No output load” trouble, connect a 2.2 kΩ resistor in parallel to the load.
- When the signaling device connected to the output in parallel to the resistor 2.2 kΩ generates undesirable sounds, reduce the resistance value.
- Add 2.2 kΩ resistors to OUT1..OUT4 if these outputs are not used.

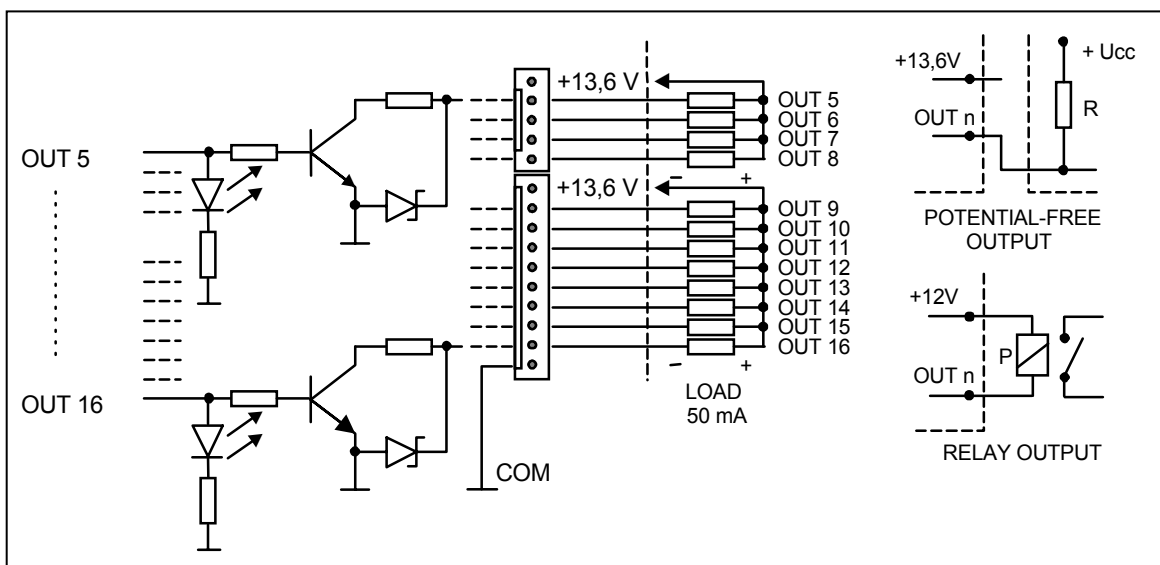


Fig. 27. Connection of loads to outputs OUT5..OUT16 and signals from these outputs (e.g. to the radio transmitter).

The remaining 12 control panel outputs are designed for control (for example, to control signaling device with their own power supply). Loads connected to these outputs (e.g. relays)

cannot force the current flow exceeding 50 mA. Structure of OUT5..OUT16 outputs and their use are shown in Figure 27.

Note: Power supply at connectors J22 and J23 is connected to power supply outputs for expanders at the control panel board. Hence, it is not advisable to connect to it any equipment exposed to tampering (e.g. signaling devices with their own power supply).

5.6 CONNECTION OF TELEPHONE LINE

If the system uses the control panel telephone communicator (for monitoring, messaging or remote programming), it is necessary to connect telephone line to the control panel. The telephone line is plugged to the terminal located in upper right corner of PCB. In order to ensure correct messaging, the control panel must be connected directly to the telephone line (terminals marked TIP, RING), and all other equipment (telephone set, fax) – downstream the control panel (terminals marked T-1, R-1). Such connection allows the control panel to fully capture the telephone line for the time of calling, which prevents the possibility of the messaging function to be blocked by picking up the handset. Additionally, the telephone sets connected behind the control panel do not signal phone calls made by the control panel.

The telephone line must be made with a four-wire cable so that the control panel can be connected before the remaining equipment (telephone, telefax, etc.).

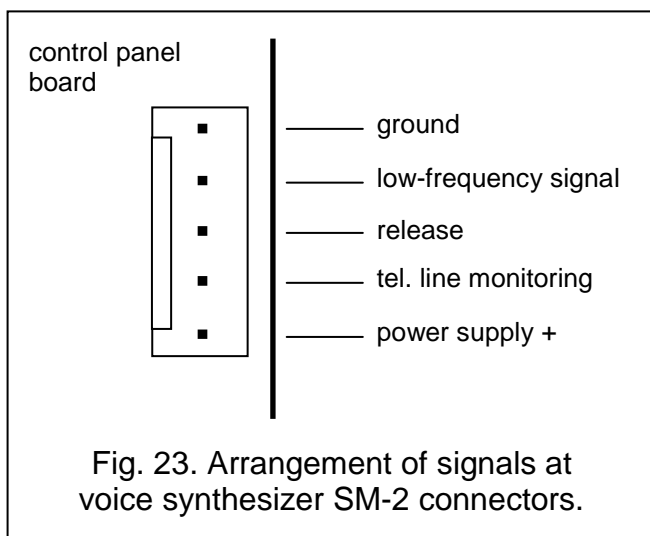


CAUTION!

- Do not send telephone signals and alarm system signals by one multicore cable. This may result in a damage to the system in case of a high-voltage punch-through from the telephone line.
- Telephone terminals of the panel should be connected to PSTN lines only. Connecting to ISDN lines may lead to damage of the equipment.
- The system installer should provide the user with necessary information on how the control panel should be connected to the telephone network.

5.7 CONNECTION OF VOICE SYNTHESIZERS

In the event the function of messaging on alarm by phone with a voice message is used, it is necessary to connect at least one voice synthesizer to the control panel.



The CA-64 control panel is provided with two sockets for connecting SM-2 voice synthesizers. Both sockets are located at the right side of PCB, between telephone line connector and J22 and J23 output sockets. The SYNT1 marked socket is used for connection of the *Synthesizer 1* message, and SYNT2 – for the *Synthesizer 2* message. Playback of the message and "monitoring" of the telephone line are possible on both SM-2 synthesizers.

When a larger number of messages is needed, it is necessary to use the expander module type CA-64 SM. These synthesizers are controlled via the extension bus, and

audio signals are connected to SYNT1 or SYNT2 terminals.

5.8 CONNECTION OF PRINTER

The control panel RS-232 port allows connection of a printer provided with a serial port. The control panel may print events in a “compressed” format (single event is printed in a single line containing up to 80 characters) or “extended” format, with names of zones, partitions, users and modules (then, the event is printed in two lines, when the printer with up to 80 characters per line is used; the descriptions of a single event are printed in one line with printers printing 132 characters per line).

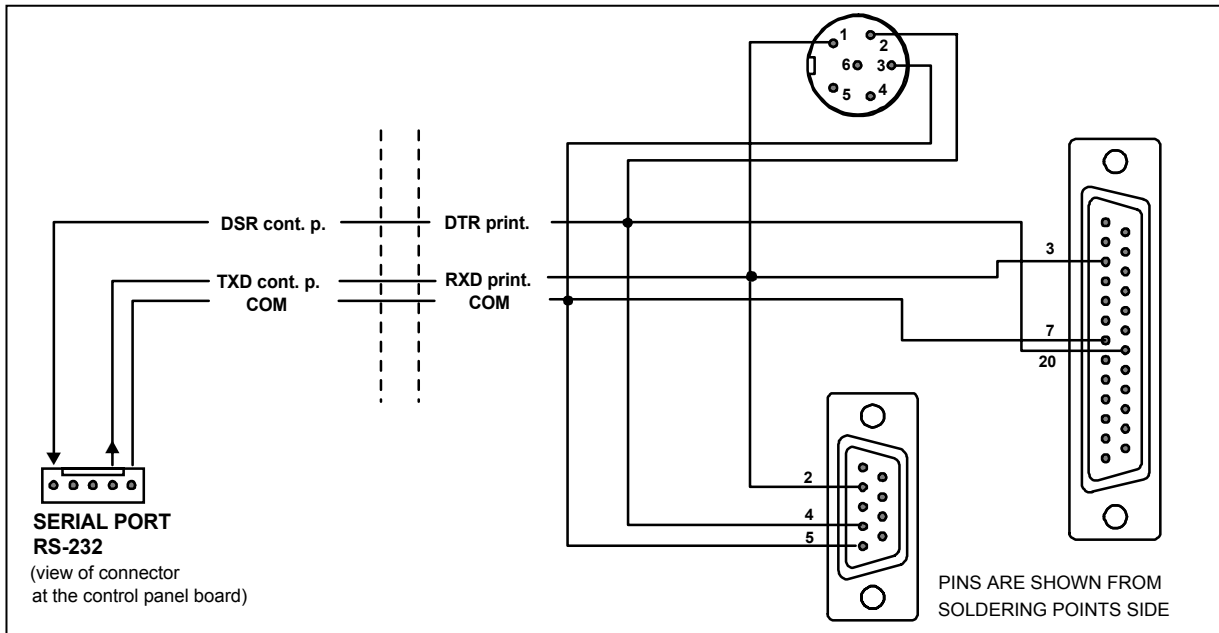


Fig. 29. Connection of a printer to the control panel serial port.

5.9 CONNECTION OF SERVICE COMPUTER

When the CA-64 control panel is programmed by means of a computer using the „Downloading” function through the panel RS-232 port, the computer must be connected as shown in Fig. 30.

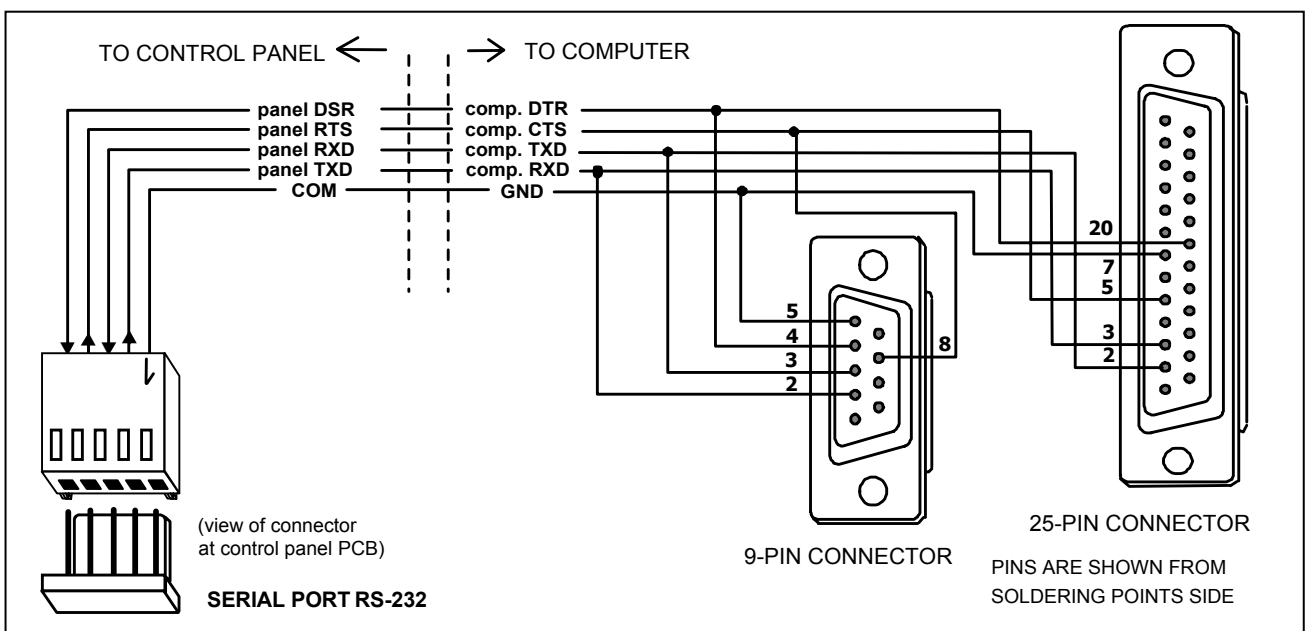


Fig. 30. Connection of a computer to the control panel serial port.



Notes:

- Do not short or touch the serial port RS-232 pins with your fingers.
- Prior to connecting the cable, the installer should remove the electrostatic charge, e.g. by touching a grounded equipment (faucet, heater, etc.) with the top of his hand.
- It is recommended that the cable be connected first to the control panel connector, and then to the computer or printer connector.

5.10 CONNECTION OF EXTERNAL MODEM AND GSM-4 MODULE

The CA-64 control panel may be programmed via the telephone line with the use of external modem. A baud rate of 300 bauds is used for programming via the modem integrated in the control panel. For this baud rate, reading of all control panel settings and programming new ones may take up to one hour. Additionally, programming via internal modem is not accessible by means of a cellular telephone (GSM or DCS) due to the baud rate established in cellular telephony.

Connecting the external modem eliminates all these limitations. A higher baud rate, when an external modem is connected, makes it possible for DLOAD64 to run at the same speed as when the computer is connected directly to the control panel (RS-232 to computer COM).

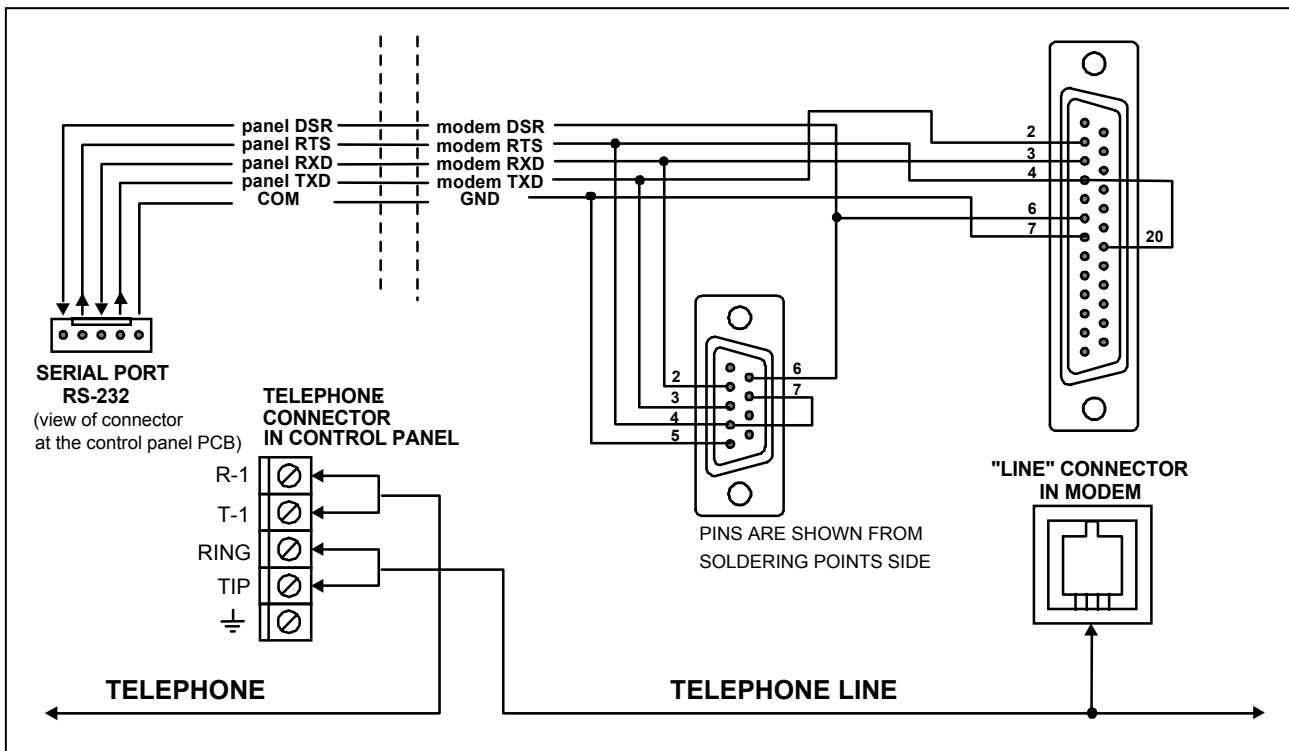


Fig. 31. Connection of an external modem to the control panel serial port.

Before being connected to the control panel, the modem needs a proper preparation: connect it to the computer and, using the *Terminal* type program, set the suitable operating mode and save its settings. You should follow the procedure below:

1. Check whether the modem is connected to the terminal – modem should answer OK after writing at↵ (if modem does not answer, try ate1↵ ; if there is no answer again, check the modem cabling to the computer and check whether COM port is properly selected in settings of the program of *Terminal* type).
2. Check the settings of parameters determining modem operation mode. After the command at&v↵, modem shows the list of parameters for programming. Setting of just few parameters is important for correct operation of the control panel – in the parameter block

stored as “profile 0” („STORED PROFILE 0” in Figure 32) it must be specified E1 Q0 V1 X4 &D2 &S0 and S00:000.

3. If the parameters mentioned above are set correctly, the modem is ready for operation with the control panel. If any parameter is set to other value, set it properly. Command for parameter setting consists of fixed prefix AT and parameter value required (for example, when profile specifies E0 V0, the command for setting the proper parameter value is `ate1v1` ↵, after which the modem answers OK).

```

OK
at&v
ACTIVE PROFILE:
B1 E1 L1 M1 N1 Q0 T V1 W0 X4 Y0 &C1 &D2 &G0 &J0 &K3 &Q5 &R1 &S0 &T5 &X0 &Y0
S00:000 S01:000 S02:043 S03:013 S04:010 S05:008 S06:002 S07:050 S08:002 S09:006
S10:014 S11:095 S12:050 S18:000 S25:005 S26:001 S36:007 S37:000 S38:020 S46:138
S48:007 S95:000

STORED PROFILE 0:
B1 E1 L1 M1 N1 Q0 T V1 W0 X4 Y0 &C1 &D2 &G0 &J0 &K3 &Q5 &R1 &S0 &T5 &X0
S00:000 S02:043 S06:002 S07:050 S08:002 S09:006 S10:014 S11:095 S12:050 S18:000
S36:007 S37:000 S40:104 S41:195 S46:138 S95:000

STORED PROFILE 1:
B1 E1 L1 M1 N1 Q0 T V1 W0 X4 Y0 &C1 &D2 &G0 &J0 &K3 &Q5 &R1 &S0 &T5 &X0
S00:000 S02:043 S06:002 S07:050 S08:002 S09:006 S10:014 S11:095 S12:050 S18:000
S36:007 S37:000 S40:104 S41:195 S46:138 S95:000

TELEPHONE NUMBERS:
0=                               1=
2=                               3=

OK

```

Fig. 32. Correct setting of external modem parameters.

4. After parameter values are set according to the list described in point 2, save the settings in the “profile 0” (with command `at&w0` ↵).
5. At the end, you may check whether all parameters are stored correctly – after the command `atz` ↵, and then `at&v` ↵, settings in ACTIVE PROFILE should be the same as in STORED PROFILE 0 (note: often STORED PROFILE set contains less number of parameters than ACTIVE PROFILE set, this is normal).

Notes:

- Modem S0 register value is set with the `ats0=0` command (modem shows slightly different notation, S00:000, in Figure 32).
- When the control panel restarts the modem, it generates the ATZ command, which sets parameters in accordance with the values stored in the “profile 0”. Therefore, it is not important what are the current values of parameters mentioned in point 2 (“ACTIVE PROFILE”), but it is important that they be correctly set in the “profile 0”.

The CA-64 control panel with software in version 1.04.03 (or later) can interact with ISDN type modem and GSM-4 communication module.

In order to start communication through the **ISDN modem** you should:

- Enter the control panel settings and select the options: „External modem” and „ISDN/GSM modem” (Service mode → Options → Tel. options →).
- Connect, using a suitable cable, the panel RS-232 port to the modem port (Fig. 31).
- The modem analog output, if any, may be connected to the control panel terminals TIP, RING.

- Program the ID codes and numbers of the control panel / computer telephones – these data must be exactly the same in the control panel and in the data file created for the control panel to be programmed.
- Initialize the modem operation and start establishing telephone connection.

Notes:

- *The control panel ISDN modem can only be used when an ISDN modem is also present on the computer side.*
- *When the connection is initiated from outside (via the telephone line), the ISDN modem will only send the ringing signal to the control panel through the RS port.*
- *Interaction with the ISDN modem does not preclude using the panel internal analog modem. If the connection is initiated from outside by an analog modem, the ringing signal is passed to the ISDN modem analog output, if any, and the call can be answered by the control panel.*
- *The „Double call” option is only valid for an analog modem.*

To start programming through the **GSM-4** module as an external modem you should:

- Select the options: „External modem” and „ISDN/GSM modem” in the panel settings.
- Connect, using a suitable cable, the panel RS-232 port to the GSM-4 module. The cable connection between the two ports is shown in the drawing below.

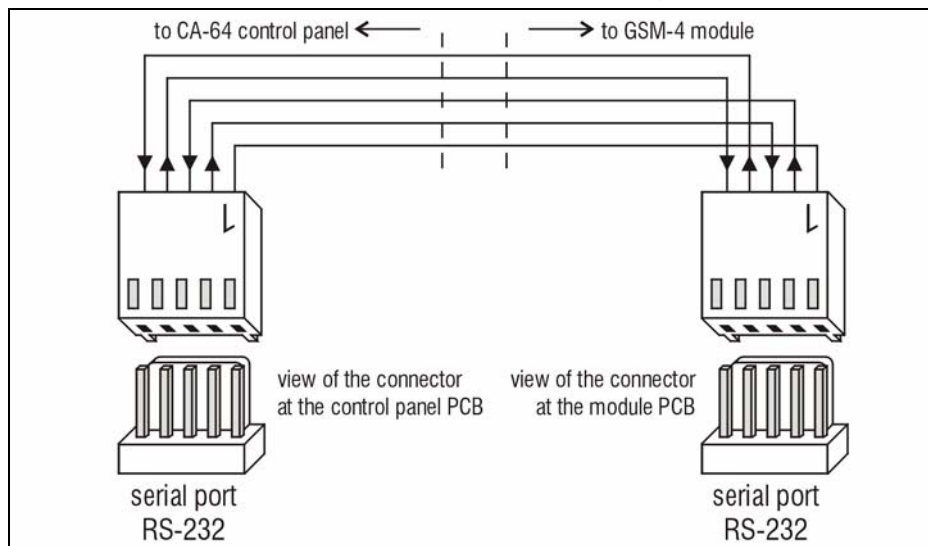


Fig. 33. Connection of RS-232 ports of CA-64 panel and GSM-4 module.

- Program corresponding functions in the GSM-4 module to make interaction with the CA-64 panel possible (control codes, computer modem format, RS rate) according to the GSM-4 user instructions.
- Program the ID codes and numbers of the control panel / computer telephones – these data must be exactly the same in the control panel and in the programmed panel file. Optionally, the control panel can call back to a different computer telephone number, not the preprogrammed one. To this end, it is necessary to include the required telephone number, terminated with a dot (e.g. CODE=602123456.), after the code initializing the module operation as modem in the SMS sent to the GSM-4 module.

Note: *To operate the GUARD64 program, it is necessary to program a separate identifier and number of the computer telephone.*

- Start the program DLOAD64 or GUARD64 in the computer, initialize the modem operation and send a corresponding SMS to the GSM-4 module.

6. STARTING THE CONTROL PANEL

When correctly installed, the control panel should start after mains power supply is switched on, as described in section **Starting the system**.

The control panel with the factory software (after restart of settings) handles all keypads installed just as if they are identified. However, it does not monitor keypads tampering and their zones, and does not permit programming of keypad operation parameters – most of the service functions is unavailable until identification of keypads and expanders is completed.

When connected to the computer, it forces generation of a new data set.

Notes:

- *Hardware identification enables access to the service mode functions.*
- *If the control panel is to be remotely programmed via the telephone line, it is necessary to program telephone number of the service computer.*
- *Hardware identification and programming of the service telephone number are made with proper service functions.*

6.1 STARTING THE SYSTEM

After power-up, the control panel start takes place in two stages:

1. First, the STARTER program starts and checks the contents of the control panel program memory. During this operation, the LED adjacent to telephone line transmitter flashes and proper message is displayed on LCD keypads. When the contents of FLASH program memory is correct, the STARTER launches the program of the control panel.
2. The program the control panel starts with checking the memory of settings (RAM memory with backup battery 3.6V/60mAh). If any differences are detected, as compared with the service programmed settings, the proper settings will be restored from FLASH memory (this test is skipped when the control panel settings are not stored in FLASH memory; question about saving the settings appears when exiting the service mode). After the settings are checked, the control panel starts working.

Notes:

- *If an error in the control panel program is detected, the “Load correct program to CA-64” message appears on LCD keypad displays and the STARTER program waits for new program from the computer. Error in the program may occur only when the control panel software up-dating process has been stopped by switching power supply off.*
- *When the control panel power supply is off, removal of the MEMORY jumper clears the contents of memory of settings, user data, event memory and clock. After reconnection of power supply, the control panel only restores the memory of settings. The user data must be programmed again. The information on administrator and service codes is stored in separate EEPROM memory and is not lost after removal of the MEMORY jumper.*

6.2 SERVICE MODE

Control panel programming from LCD keypad is carried out with the use of service functions accessible from service mode menu. This mode is switched on by the service (installer) choosing the entry “Service mode” in user function menu.

How to activate the service mode (codes as for restart of settings):

1. Open service access:
 - a) type the administrator code and press [*] (press [1111][*]),

- b) select the "Service access" from the list and enter this function (key [#] or [▶]),
 - c) specify service access time (in hours) and confirm it with the [#] key.
2. Type service code and press [*] (press [12345][*]),
 3. Select the entry "Service mode" and press [#] or [▶].

Notes:

- *Service mode is indicated with the "SERVICE" LED at LCD keypads. The control panel remains in service mode until the user exits it using the "End service" function.*
- *The only zone alarms possible in service mode are 24H VIBRATION, 24H CASH MACHINE, PANIC-AUDIBLE and PANIC-SILENT.*
- *It is possible to permanently open service access to alarm system. For this purpose the "Permanent service access" option should be activated with the use of the administrator code in the "Change option" user function.*
- *If administrator has forgotten his code and service access is closed (service access time=0), the installer may enter a new administrator code (without clearing of the previously entered users codes). For this purpose, you should enter the service mode with the use of jumpers (see description below) and quit with the use of "End service" function. Within circa 20 seconds after exiting the service mode, the installer can call the "Administrators" function and enter a new code.*

If starting of the service mode according to the description above is impossible – the control panel does not control the keypad because of any reason – it is necessary to carry out special procedure to start the control panel and enter the service mode "with the use of jumpers". To ensure that all settings are in accordance with factory settings, perform functions of setting restarts in the service mode.

The procedure goes as follows:

1. Disconnect in turn the AC supply and the battery and check keypad connections to the keypad bus.
2. Set the jumper at RESET pins at the control panel PCB.
3. Connect in turn the battery and the AC supply - LED located at the telephone line transmitter starts blinking (the control panel will not start when connected to battery only).
4. Wait until LED goes off, then remove the jumper from pins – the control panel should enter the service mode menu automatically – the message "→End service" appears on the display of keypad with lowest address number, and the SERVICE LED starts blinking. If the "Clear settings? 1=Yes" message appears on the main display, this means that the access to the service mode "with the use of jumpers" has been blocked in the control panel program (→Service Mode →Configuration →Block SM). Then you can enter the Service Mode by pressing the key marked with digit 1, but, at the same time, all settings previously programmed in control panel will be cleared (just like after performing functions mentioned in point 5). After performing this operation, you may move to point 6.
5. Perform restart functions (→Restarts →Clear settings / →Clear codes / →Clear event log).
6. Perform identification functions for modules connected (→Structure →Hardware →Identification →LCD keypads id. / →Expanders id.).

Note: *The addresses in keypads and expanders cannot be changed after identification has been performed.*

7. Complete the service mode with "End service" function, saving data in FLASH memory. When the "Store settings in FLASH ? 1=Yes" prompt appears on the keypad display, press key with digit 1 – new settings will be saved and the control panel will enter the basic operation mode (waiting for code).
8. Call the service mode again.

If the control panel enters the service mode again, its operation is OK and you can proceed to further system installation (connection of expanders, detectors, signaling devices, keypads, etc.), start communication with the computer and program all parameters required.

Notes:

- *If the control panel is connected to the computer with DLOAD64 program started, function of downloading via RS-232 will be started instead of the service mode.*
- *Entering the service mode “with the use of jumpers” may be blocked with the “Block SM” function (function in “Configuration” position). Entering the service mode “with the use of jumpers” may be restored after approval of factory setting restoration.*

When exiting the service mode, the control panel CA-64 checks whether parameter values programmed by the service have changed. If there are changes in settings, the control panel asks: “Store settings in FLASH ? 1=Yes” and after pressing the [1] key new settings will be saved in memory.

In large systems, the parameters defining control panel operation are usually stored in the memory with independent battery backup.

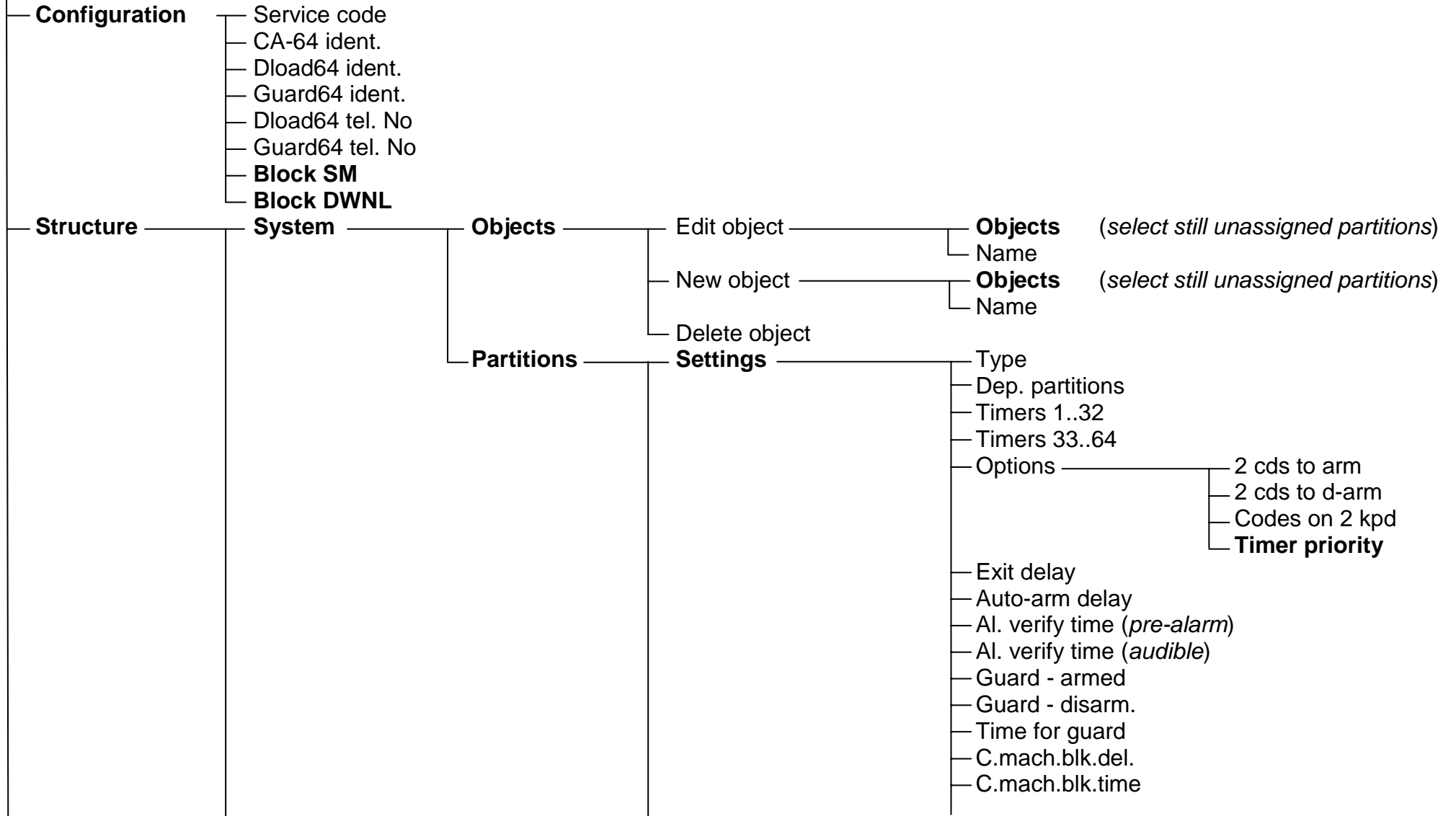
Disconnection of the memory power supply when the control panel power supply from backup battery 13.6V is switched off will cause clearing of settings. Saving the data in FLASH memory makes clearing of settings impossible and allows the control panel to restore them when an error is detected.

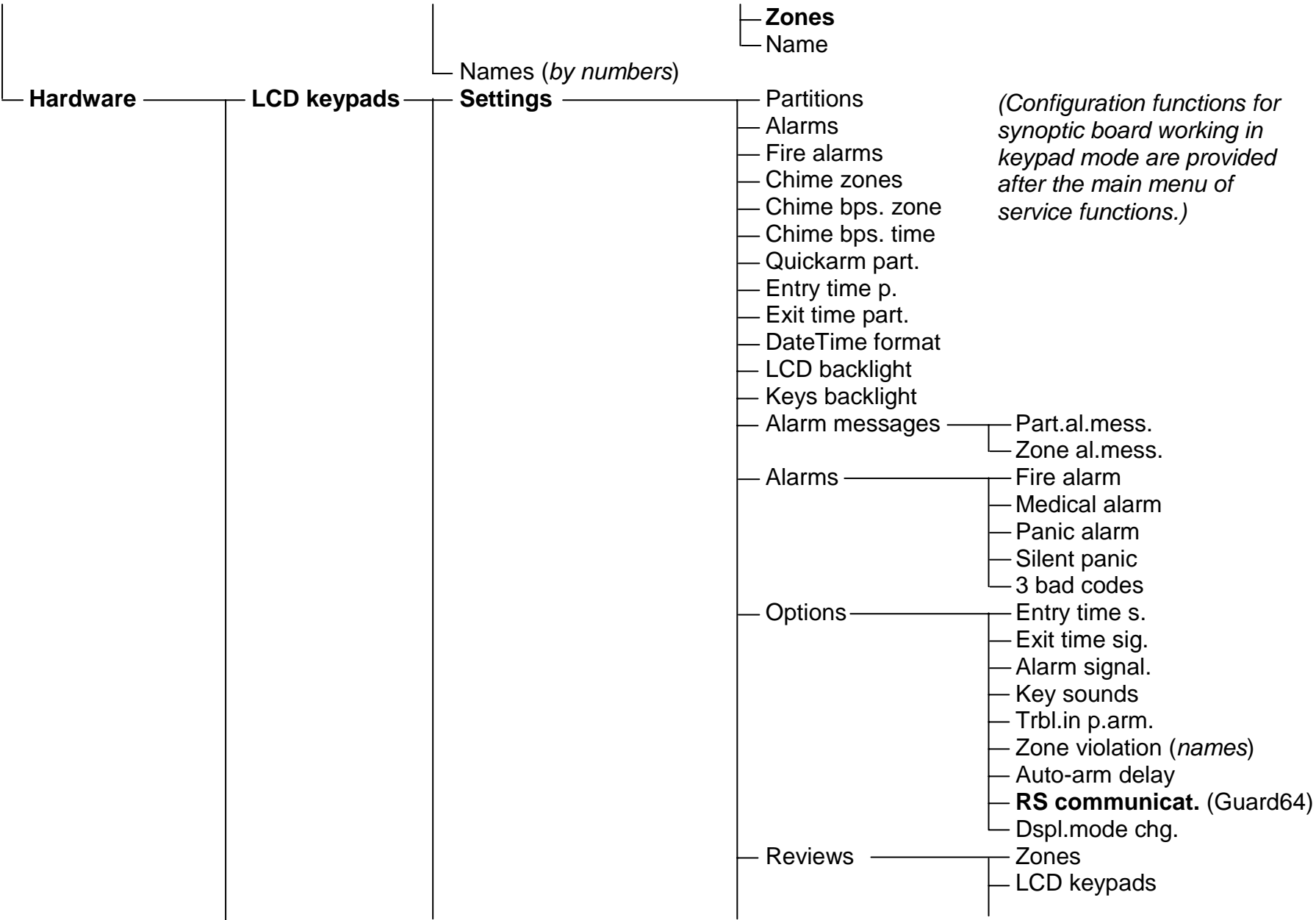
Note: *RAM memory errors should not occur in a correctly configured and properly powered system.*

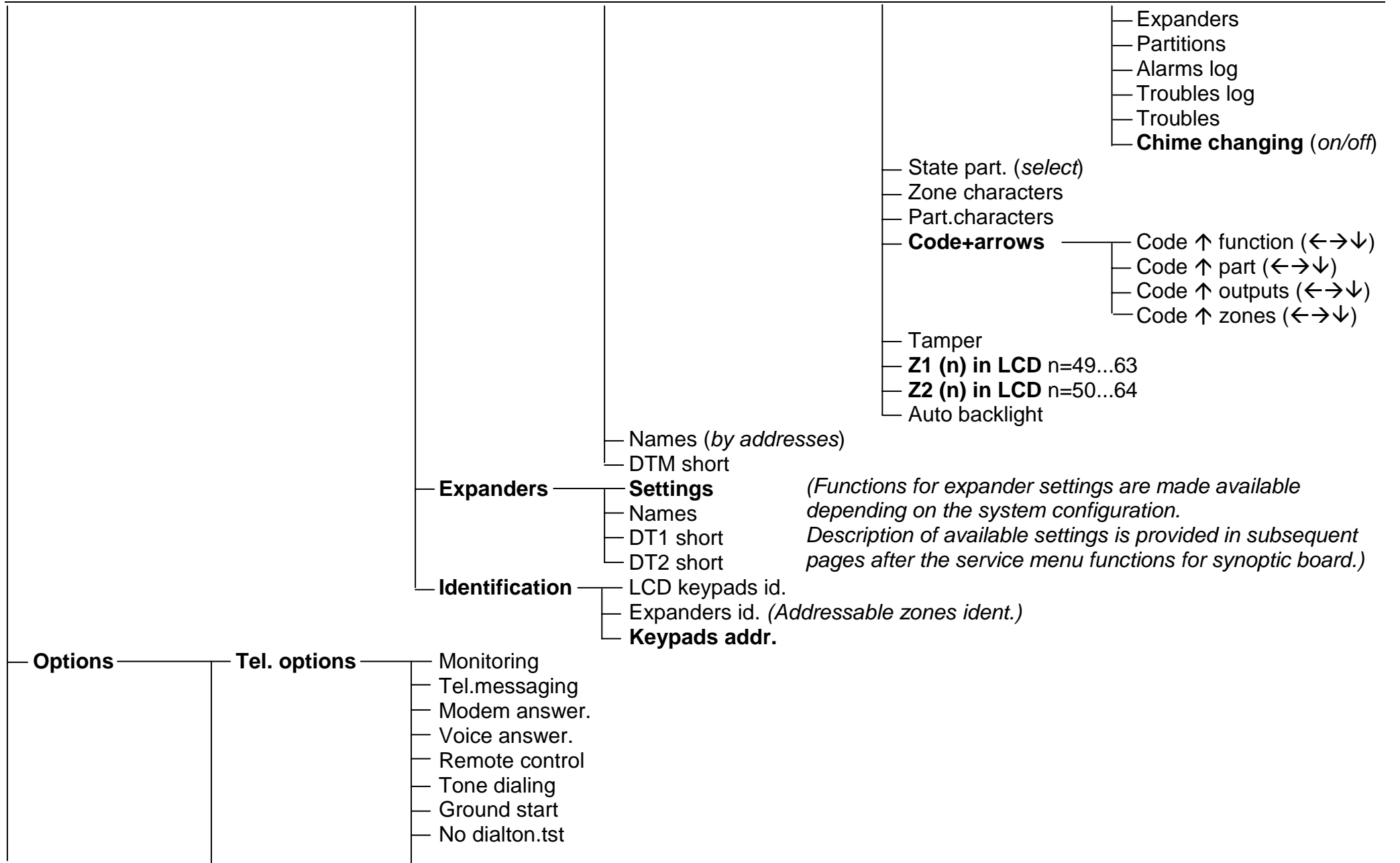
6.2.1 SERVICE MODE MENU

[SERVICE CODE][*][9] (starting the service mode with a shortcut)

→ Service end

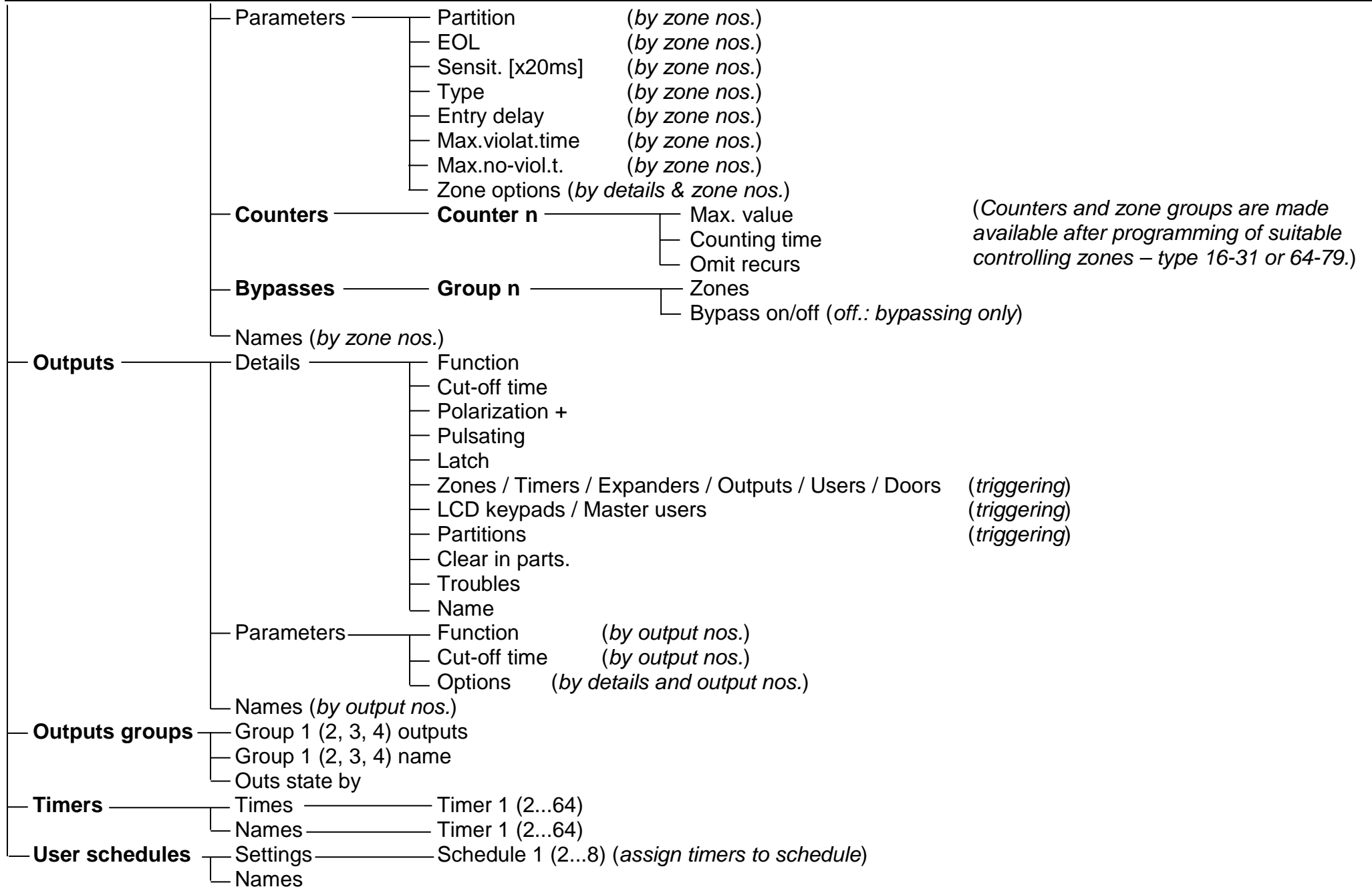


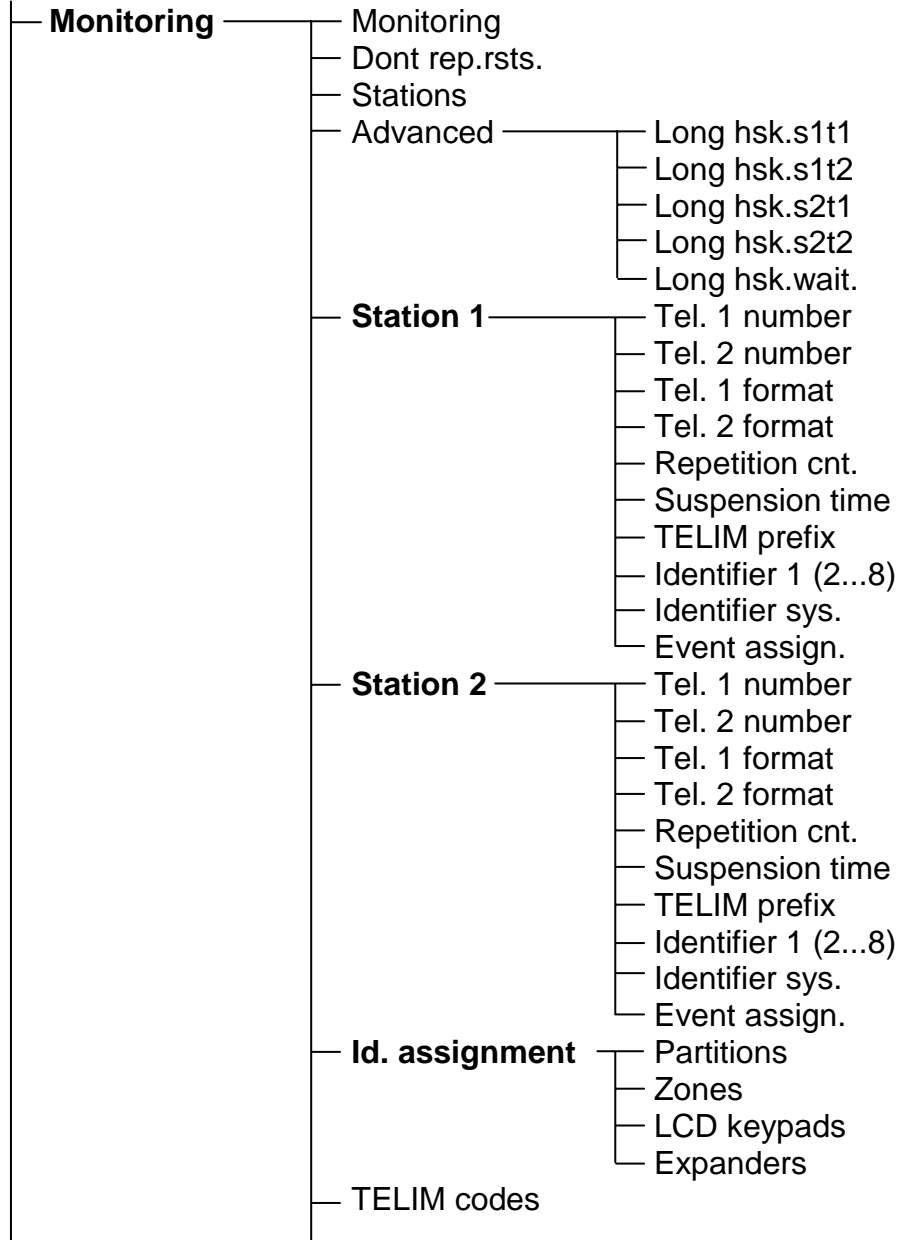




	<ul style="list-style-type: none"> — No answer test — Dbl.voice msg. — Double call — External modem — ISDN/GSM modem — Pulse 1/1.5 	
— Printer options	<ul style="list-style-type: none"> — Printing — Monitor.status — Names/descript — Wide paper — 2400bps (<i>off: 1200 bps</i>) — CR+LF (<i>off: CR</i>) — Parity bit — Parity: EVEN (<i>off: ODD</i>) — Zone alarms — Part/mod. al. — Arming/disarm. — Bypasses — Access control — Troubles — User functions — System events 	
— Active rights		(<i>see: USER MANUAL – USERS function</i>)
— Various options	<ul style="list-style-type: none"> — Simple codes — Notify of code — Confirm with 1 — Autoabort msg. — SM -> menu — Tests -> menu — Fast exp. bus — No rest. mon. — Inf.aft.tamper — No BATT,no arm — Exp.trb.no arm — Arm, trb.warn. — Zones bef. arm 	<ul style="list-style-type: none"> (<i>cancel messaging together with alarm clearance</i>) (<i>reset</i>) (<i>reset</i>) (<i>fast data transmission on expander buses</i>) (<i>do not monitor module restarts</i>) (<i>display message after tamper alarm until service intervention</i>) (<i>do not arm during battery trouble</i>) (<i>do not arm during expander trouble</i>) (<i>warn of troubles before arming</i>) (<i>view violated zones before arming</i>)

<ul style="list-style-type: none"> — Times — Rings to answer — Prefix length — Clock adjustm. — Daylight saving — Summer time — Winter time — Zones 	<ul style="list-style-type: none"> — Global entry delay — Global alarm time — AC loss report delay — Tel. loss report delay — Details — EOL — Sensit. [x20ms] — Type — Entry delay / Alarm delay / Surveillan.time / Signal. delay / Bypass time (64-79) / Expander number (58) — Max.viol.time / Max.opening t. (for 57 type zones) / Arming mode (80, 82) — Max.n-viol.time — Partition — Power up delay — Priority / Disrm.on viol. (for 82 type zones) — Outputs chime — Video,disarmed — Video,armed — Bypass disabl. — Bypass no exit — Bell delay / Alarm if armed (for 64-79 type zones) / Clear alarm (for 81, 82 type zones) — Auto-reset 3 — Auto-reset 1 — Auto-rst. clr. — Pre-alarm — Abort delay / Part.tmp.block (for 84 type zones) — Rest.aft. bell — Rst.aft.disarm — Al.on exit end (when violat.) / Violat.events (47) / No bp.if armed (64-79) / Abort voice m. (81, 82, 83) — Al. aft.unbps. (alarms when violated after unbypassing) — Name
--	---





Event codes

Identifier 1 (2...8)

Zones

- Alarm
- Restore
- Tamper
- Tamper rst.
- Trouble
- Trouble rst.
- Bypass
- Unbypass
- Violation

Partitions

- Arm
- Disarm
- Clear alarm
- Duress alarm
- Defer autoarm
- No guard

LCD keypads

- Panic alarm
- Fire alarm
- Medical alarm
- Tamper
- Tamper rst.
- Unauthorised
- 3 bad codes

Expanders

- Panic alarm
- Fire alarm
- Medical alarm
- Tamper
- Tamper rst.
- Unauthorised
- 3 bad codes

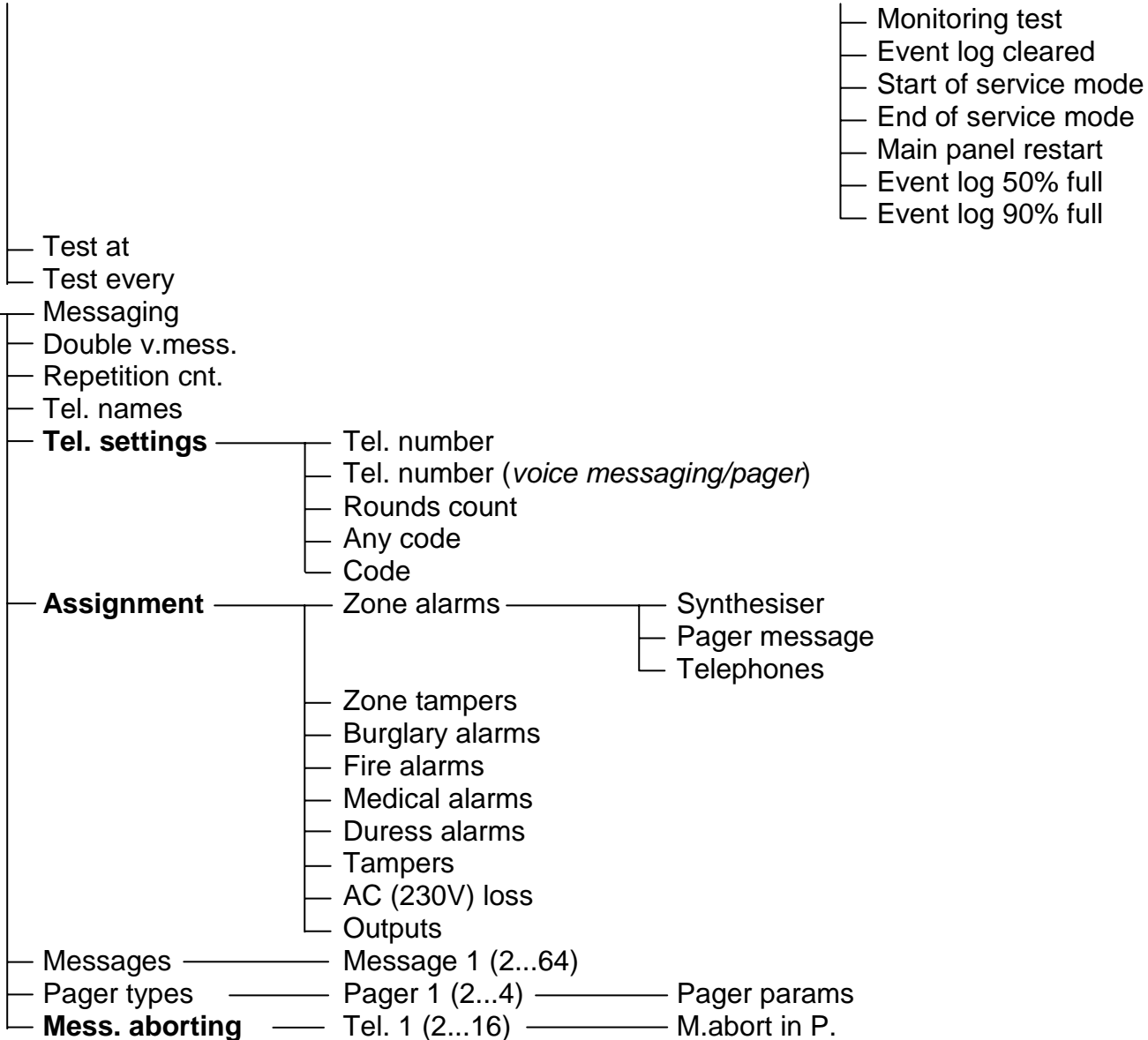
Identifier sys.

Troubles

- AC (230V) loss
- Battery trouble
- Settings clear
- Monitoring trouble
- Fire zones test

			<ul style="list-style-type: none">— Burglary zones test— Real-time clock trouble— OUT1 trouble— OUT2 trouble— OUT3 trouble— OUT4 trouble— LCD keypads supply trbl.— Expanders supply trbl.— DTM bus trouble— DT1 bus trouble— DT2 bus trouble
		Troubles rst.	<ul style="list-style-type: none">— AC (230V) ok— Battery ok— Settings restore from FLASH— Monitoring ok— Fire zones test finished— Burglary zones test finished— Real-time clock setting— OUT1 ok— OUT2 ok— OUT3 ok— OUT4 ok— LCD keypads supply ok— Expanders supply ok— DTM bus ok— DT1 bus ok— DT2 bus ok
		Other	<ul style="list-style-type: none">— RAM memory error— Call back— DWNL finished— Unsuccessful DWNL attempt— Manual test of monitoring— Periodical test of monitoring

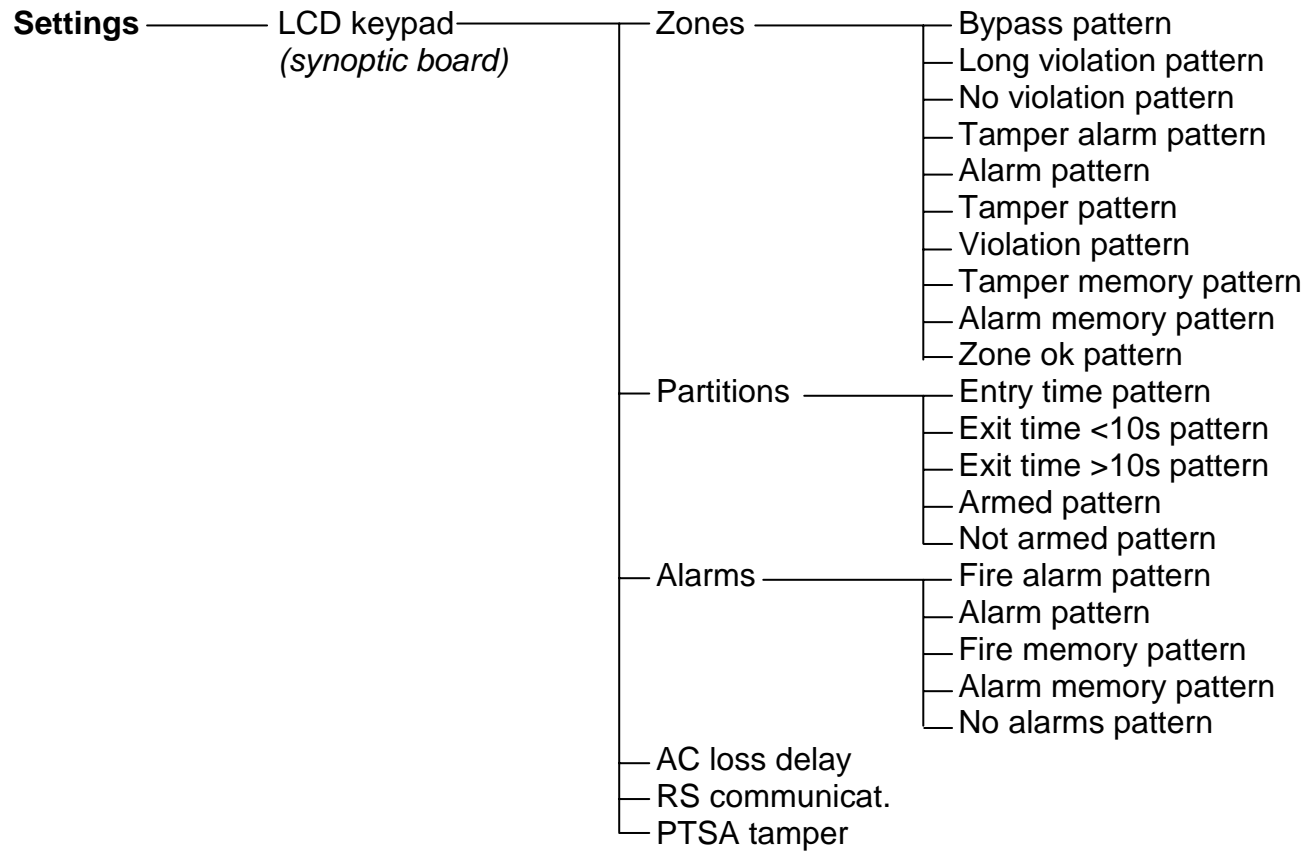
Messaging



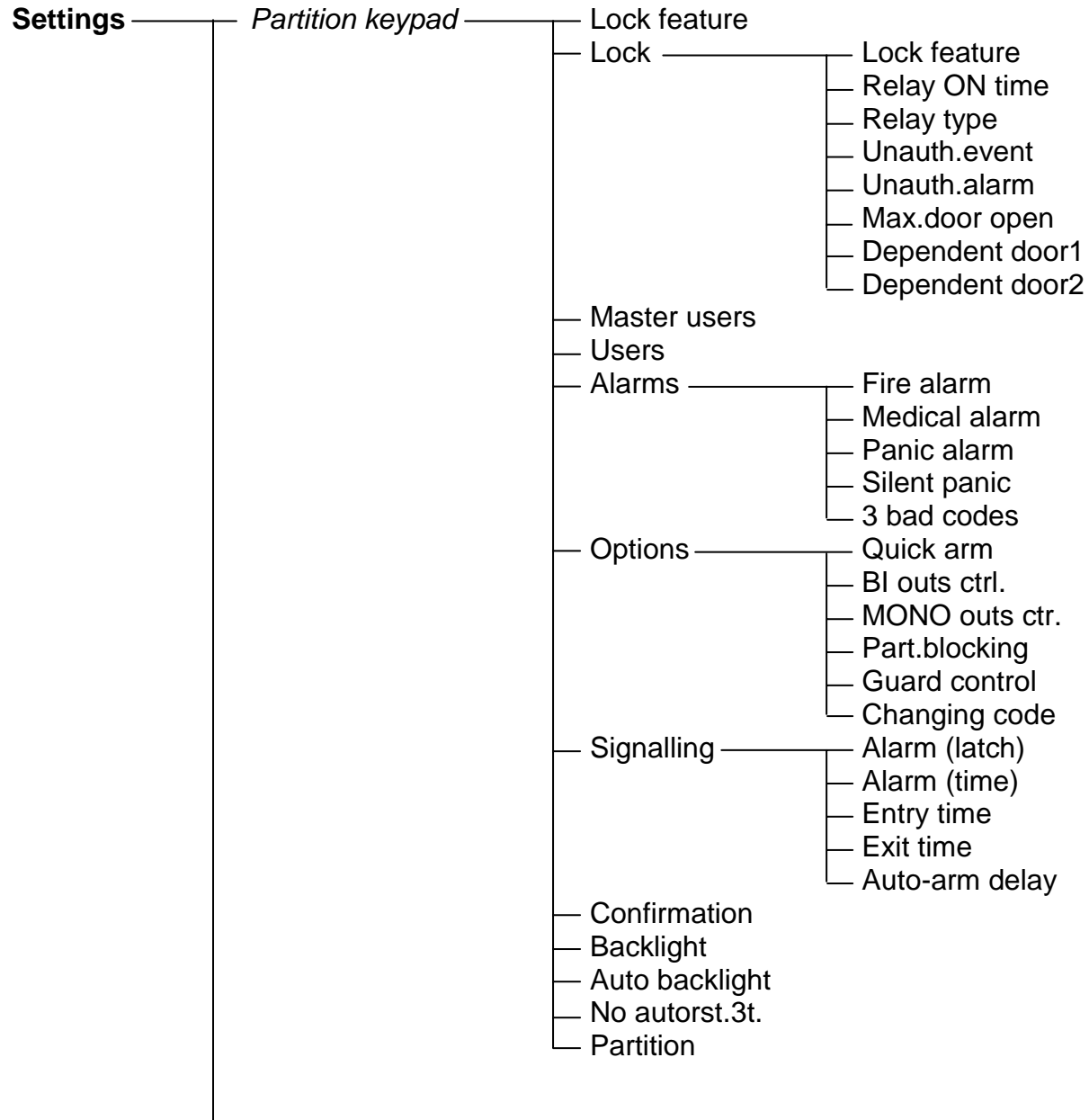
- Monitoring test
- Event log cleared
- Start of service mode
- End of service mode
- Main panel restart
- Event log 50% full
- Event log 90% full

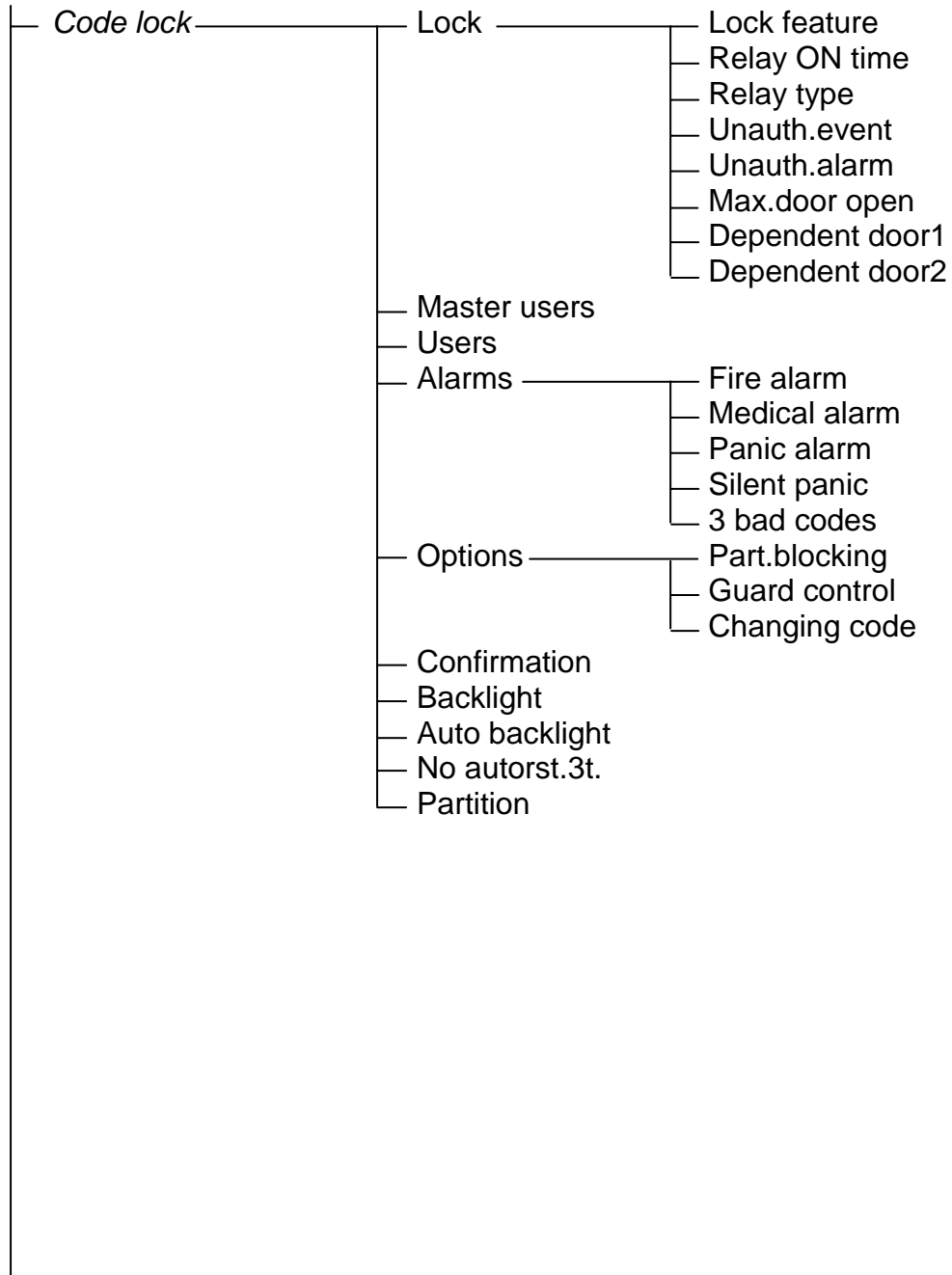
Tel.answ./ctrl.	Answering
	Double call
	Rings count
	On armed part. (<i>select partitions</i>)
	Remote control
	Users (all) (<i>assign remote switches to control</i>)
	Users (t.code) (<i>assign remote switches to control</i>)
Note	Text
	Valid (<i>days</i>)
	From (<i>date</i>)
	For (<i>select user</i>)
	Who can erase (<i>select user</i>)
System status	Partitions
	Zones
	LCD keypads (<i>tamper</i>)
	Expanders (<i>tamper</i>)
	Troubles
	Supply voltage
Restarts	Clear all
	Clear settings
	Clear codes
	Clear event log
	Settings<-FLASH
	Starter

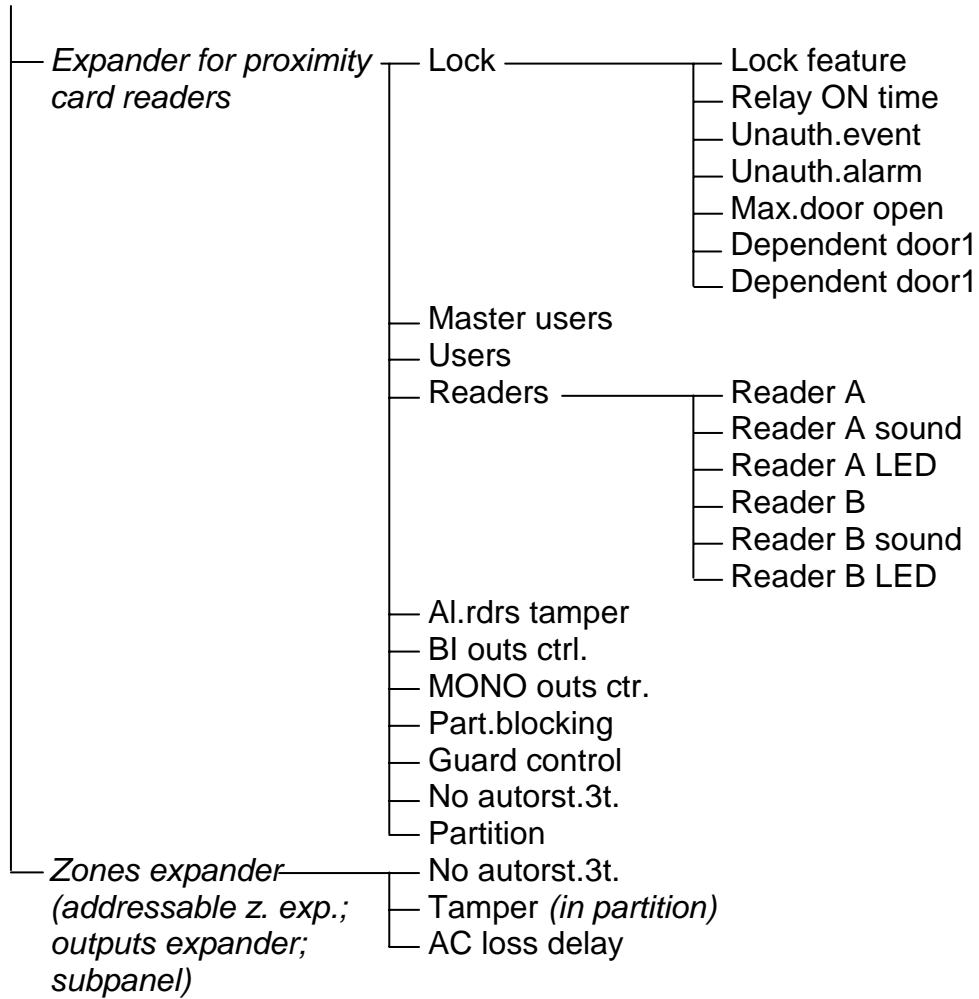
Menu of service functions for a **synoptic board** working in keypad mode (→Structure →Hardware →LCD keypads →Settings).



Menu of service functions for particular **expanders** (→Structure →Hardware →Expanders →Settings).







6.3 CONTROL PANEL PROGRAMMING

The most convenient way of the control panel programming is by means of the computer via the RS-232serial port. The program which is needed for that, i.e. the DLOAD64.EXE, is delivered together with the control panel. Connect the control panel with computer as shown in Figure 30. Data exchange is carried out after download function is activated. This function is called by the service (installer) from user menu. If restart of control panel settings has already been made (factory settings), proceed as follows:

1. Open service access:
 - a) type administrator code and press [*] (press [1111][*]),
 - b) select the "Service access" item from the list and enter this function (key [#] or [▶]),
 - c) specify service access time (in hours) and confirm it with key [#]
2. Type service code and press [*] (press [12345][*]),
3. Select the position "Downloading" from the list and press key [#] or [▶],
4. Position "Start DWNL-RS" appears on the display - press key [#] or [▶].

Notes:

- *The control panel remains in downloading function until it receives the "Terminate communication" command from the computer (the last item of "Communication" menu) or until it exits the function due to the "Finish DWNL-RS" command. The last command appears in user function menu in "Downloading" item when the function menu is called by the service.*
- *After the DLOAD64 program is started in the computer connected to the control panel, communication starts automatically. The window showing which system is communicated with appears on the screen.*
- *To protect data, the CA-64 allows disabling of the downloading function "with the use of jumpers". The "Block DWNL" service mode function (in „Configuration" menu) is used for that.*
- *The control panel stores and makes available to the user the date and time of saving the data in the panel as well as the file name in the DLOAD64 program (user function: TESTS→File in Dload64).*

The downloading function starts automatically when the control panel is connected via RS-232 to the computer in which DLOAD64 is started, then the function switches on the control panel power supply.

6.4 PROGRAMMING BY TELEPHONE

When restart with restoration of factory settings is already made for the control panel, the telephone number of service computer must be programmed to start programming. Proceed as follows:

1. Enter the service mode,
2. Select position "Configuration",
3. Select position "Computer telephone",
4. Program the computer telephone number (0..9 – digits, B – switch over to pulse dialing, C – switch over to tone dialing, D – waiting for additional signal, E – 3-second pause, F – 10-second pause, * # a b c d – signals additionally generated in DTMF mode).

Programming of special characters in telephone number using LCD keypad:

- enter a digit (in accordance with the table) in place of the special character

- press [▼] key – the blinking cursor appears (big rectangle)
- move the cursor back (key [◀]) to show entered digit and press again key with this digit – the proper special character will appear
- enter DTMF special characters designated with small letters “abcd” by using key with digit 8 by repeatedly calling the above mentioned selection procedure.

Special character	Function description	Key with digit
A	end of number	0
B	switch over to pulse dialing	1
C	switch over to tone dialing	2
D	waiting for additional signal	3
E	3-second pause	4
F	10-second pause	5
*	signal * in DTMF mode	6
#	signal # in DTMF mode	7
a b c d	other signals generated in DTMF mode	8

Note: Do not program the “A” character for a telephone number (A is a marker of number end), as it is automatically added after the last digit.

Start of communication with the computer via telephone line is ensured by “Start DWNL-TEL” function. This function is accessible in the user functions menu for the administrator and the service (if the service personnel are authorized to start downloading).

7. BASIC TECHNICAL DATA

Mainboard supply voltage	AC 20...24V
Control panel current consumption	120mA
Nominal power supply unit voltage	13.6 – 13.8 V
Power supply unit output current.....	3A
LCD keypad current consumption, min. / max	60/125mA
Output OUT1 ... OUT4 load	3A
Output OUT5 ... OUT16 load	50mA
Output +KPD load.....	3A
Output +EX1 and +EX2 load.....	totally 3A
Battery charging current.....	switched 500/1000mA
Ambient temperature	0...+55°C

Table 1. Example of panel power supply load estimation / battery selection.

No.	Loads	Max current	Mean current consumption
1	Mainboard CA-64	120mA	120mA
2	LCD Keypad and 16 detectors*	445mA	300mA
3	Output OUT1...OUT4	4 x 3A	6A
4	Outputs OUT 5...OUT16	12 x 50mA	300mA
5	Battery charging current	500mA/1000mA	-
Total max current consumption by the system with no alarm signaling		$\Sigma I = 120\text{mA} + 445\text{mA} + 600\text{mA} + 1000\text{mA} = 2170\text{mA}$	
Battery selection based on max. and mean current consumption by the system, assumed duration of power failure 12h, assumed 1 alarm with 15 min (0.25h) duration of signaling		$\Sigma A_{\text{Max}} = 1.25 \times (0,12 \times 12 + 0,445 \times 12 + 12 \times 0,25 + 0,6 \times 0,25) \approx 12,4\text{Ah}$ $\Sigma A_{\text{Av}} = 1.25 \times (0,12 \times 12 + 0,3 \times 12 + 6 \times 0,25 + 0,3 \times 0,25) \approx 8,3\text{Ah}$ Recommended standby power supply: battery 12V/17Ah	

* Assumed current consumption by a single detector 20mA.

** When the capacity of the power supply is exceeded, the current is supplied by battery.

Notes:

- *The control panel power supply unit has been designed for work with lead batteries or other batteries with a similar charging curve (European Directives 91/157/EEC and 83/86/EEC).*
- *It is impermissible to connect a fully discharged battery (with voltage on unloaded terminals less than 11V) to the alarm panel. To avoid hardware damage, fully discharged or never used battery should be precharged with the use of a proper charger.*



8. HISTORY OF THE MANUAL UPDATES

Shown below is a description of changes made to the contents of this manual as compared with that drawn up for the control panel with program version v1.04.02.

DATE	FIRMWARE VERSION	DESCRIPTION OF CHANGES
March 2004	1.04.03	<p>Information on RS-232 interface has been supplemented (p. 4).</p> <p>Description of synoptic board has been added (p.).</p> <p>Information on creating a new object has been supplemented (p. 9).</p> <p>Description of settings for partitions (p. 8), zones (str. 12) and outputs (p. 18) has been added. Functioning of "Partition user's timer" has been improved (p. 10); new zone options have been added; viewing violated zones prior to arming has been made possible (without PRIORITY option) (p.).</p> <p>Description of temporarily blocked partition has been supplemented (p. 9).</p> <p>Remark on using the "Active authority" function has been added (p.).</p> <p>Operations necessary to start messaging (p.), telephone control (p. 31) and LCD keypad control (p. 32) have been described.</p> <p>Information on programming the control panel through GSM-4 module has been added (p. 32).</p> <p>Section "Keypad connection" (p. 37) has been updated.</p> <p>Permanent display of the keypad name has been made possible (p. 42 clock format).</p> <p>Information on connecting to the control panel of ISDN modem (p. 51) and GSM-4 module (p. 52) has been added.</p> <p>Section "Starting the control panel" (p. 53) has been updated.</p> <p>Service mode MENU has been included (p. 56).</p> <p>New options have been added (zones and system).</p> <p>Function „File in Dload64" has been added (p. 71).</p> <p>Drawings of DLOAD64 program windows (version 1.04.03), and drawings of hardware connection to RS-232 port have been updated.</p>
July 2004	1.04.04	<p>List and descriptions of parameters (p. 12) and zone options (p. 13) have been updated.</p> <p>Description of output triggering methods (p. 19) has been updated.</p> <p>New type of output: „Tamper alarm" (p. 23) has been added.</p> <p>Section "Answering a phone call" has been modified (p. 31).</p> <p>Information on programming by means of GUARD64 program (p. 32) has been supplemented.</p> <p>Description of keypad parameters and options (p. 40) has been supplemented.</p> <p>Service mode menu (p. 56) has been supplemented.</p>

ATTENTION !

An efficient security system does not prevent burglary, assault or fire from happening, however it diminishes the risk that such a situation will cause no alarm or notification.

Therefore, the SATEL Company recommends that operation of the whole security system be regularly tested.

SATEL sp. z o.o.
ul. Schuberta 79
80-172 Gdańsk
POLAND
tel. + 48 58 320 94 00
info@satel.pl
www.satel.pl