Roger Access Control System

MC16 Operating Manual

Product version: 1.1

Firmware version: 1.7.4 and newer

Document version: Rev. E

$C\epsilon$

rcdr306

roger

1. DESIGN AND APPLICATION

MC16 is access and building automation controller dedicated to RACS 5 system. The controller is offered in multiple versions and its functionalities are determined by license file on its memory card. The MC16 is offered as individual controller or within MC16-PAC-KIT which facilitates the installation and design of RACS 5 system. After the connection of MCT readers and MCX expanders, the controller can be applied in access control, Time&Attendance, hotel and building automation. The MC16 can control doors, elevators, lockers (cabinets) and car parks. The controller offers advanced and efficient methods for management of users and their authorisations (rights). The configuration of controllers in a system is performed concurrently via LAN/WAN and the total number of controllers does not affect configuration time. The controller is managed with VISO software which enables operation with centralized Microsoft SQL Server database. The system can be managed from multiple workstations with VISO software by operators with various rights. The communication with MC16 controllers in LAN/WAN is encrypted according to AES128 CBC.

Characteristics

- Access controller in RACS 5 system
- 8 inputs NO/NC
- 6 transistor outputs 15VDC/150mA
- 2 relay outputs 30V/1,5A DC/AC
- 18VAC, 12VDC and 24VDC power supply
- Built-in 12VDC/1,2A power supply unit
- Backup battery charging and monitoring
- Ethernet communication interface
- Encrypted data transmission (AES128 CBC)
- Peripheral devices interfaces: RS485, RACS CLK/DTA, Wiegand
- 8 million event buffer on memory card

Power supply

MC16 controller can be supplied from 230VAC/18VAC transformer with minimal power output 20VA, from 12VDC PSU or from 24VDC PSU. The connection of power supply is shown in fig. 1.

If MC16 controller is supplied with 18VAC or 24VDC, then 12V backup battery can be connected in order to provide power supply in case of mains supply shortage.

The controller charges backup battery with 300 mA stabilized current up to 13.8V. Backup power supply is activated automatically in case of main powers supply shortage. If the voltage at backup battery drops below approx. 10V then the battery is automatically disconnected from MC16 and remains disconnected until mains power supply returning.

In case of 12VDC power supply, backup battery cannot be directly connected to MC16 and in such case backup power supply must be provided by 12VDC power supply unit. In case of maximal load at supply outputs AUX (1A) and TML (0.2A), the controller requires 20W power.

Note: It is recommended to install MC16-PAC controllers within MC16-PAC-KITs which include power supplies for the controller and door devices. More information on kits power supply is given in their manuals.
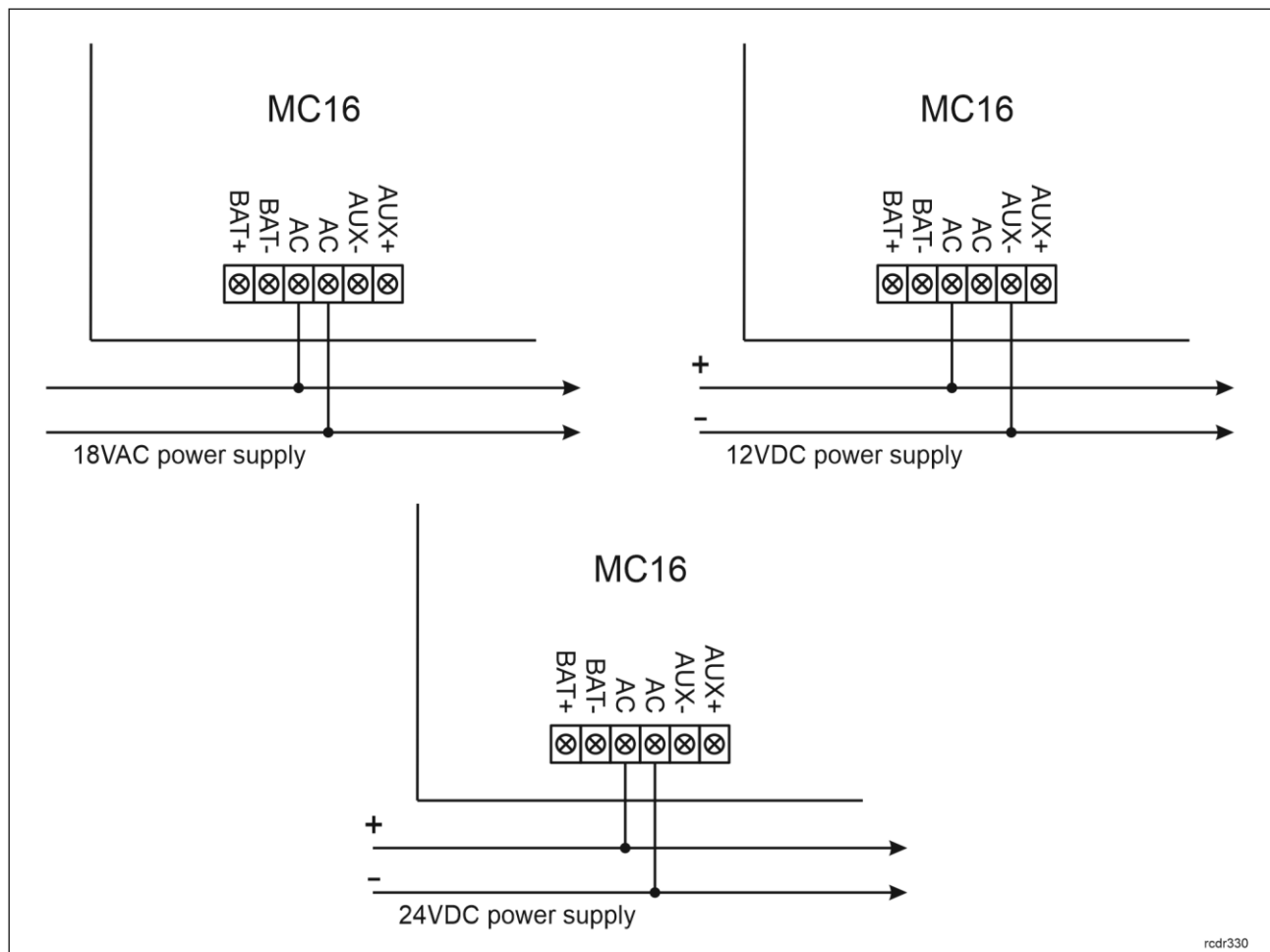
Fig .1 MC16 power supply

Ethernet interface

The communication between MC16 controller and PC is provided via LAN/WAN and it is encrypted according to AES128 CBC. Communication key is defined by system operator. Factory default IP address of controller is 192.168.10.213 and it can be changed with RogerVDM software within low level configuration.
In case of controller with firmware 1.7.4 or newer the device supports DHCP if the parameter DIP=1 is defined in DEBUG.CFG file on MC16 memory card. In such scenario the controller applies dynamic IP address instead of static IP address which is configured within low level configuration. In both cases the IP address of controller must be entered manually on the level of VISO software.

Note: The device has an Ethernet network communication interface. In principle, the device can be used in both WAN and LAN, while the manufacturer's warranty is covered only for operation in an isolated LAN reserved exclusively for the access control system or other system in which the device is to be used.

RS485 interface

The communication of MCT and MCX series peripheral devices with MC16 access controller is provided by RS485 bus which can encompass up to 16 of such devices, each with unique address in range of 100-115. The bus topology can be freely arranged as star, tree or any combination of them except for loop. The matching resistors (terminators) connected at the ends of transmitting lines are not required. In most cases communication works with any cable type (standard telephone cable, shielded or unshielded twisted pair etc.) but the recommended cable is unshielded twisted pair (U/UTP cat.5). Shielded cables should be limited to installations subject to strong electromagnetic interferences. The RS485 communication standard used in the RACS 5 system guarantees proper communication in a distance of up to 1200 meters as well as high resistance to interferences.

Communication protocol on RS485 bus of MC16 controller is a proprietary algorithm which offers encrypted and authenticated communication.

Note: Do not use more than single pair in UTP cable for RS485 communication bus.

OSDP interface

OSR series OSDP readers and third party OSDP readers can be connected to RS485 bus of MC16 access controller via MCI-3 and MCI-3-LCD hardware interfaces. Each MCI-3 can be operated with up to two OSDP readers (except for OSR88M-IO readers) configured with ID=0 and ID=1 addresses. MCI-3-LCD can be connected with single OSDP reader equipped with display (e.g. OSR88M-IO). MCI-3 type interfaces are usually installed in MC16 controller metal box. OSDP bus can be executed with unshielded twisted pair cable (U/UTP cat.5) with maximal length of 1200m.

RACS CLK/DTA interface

RACS CLK/DTA interface can be used for communication of controller with older type PRT series terminals. Up to 4 such devices can be operated via RACS CLK/DTA interface, each with unique address in range of 0-3. Prior to connection of PRT readers it is necessary to make low level configuration of the MC16 and activate the operation with such readers.

Note: If access controllers are installed in the system which must conform to the requirements of grade 3 according to EN 60839 standard then the RACS CLK/DTA bus of peripheral devices must be specifically protected mechanically against unwanted tampering. Cables of the bus cannot be accessible to strangers and they must be installed in the area protected by the access control system. Cables must be hidden and/or laid in protective ducts (preferably metal ones). Cables cannot be easily distinguishable from other cables installed inside building.

Wiegand interface

Wiegand interface can be used for communication of controller with third party readers. The communication is performed via controller inputs (IN1-IN8) and up to 4 Wiegand readers can be operated by MC16 controller. Prior to connection of Wiegand readers it is necessary to make low level configuration of the MC16 and activate the operation with such readers. Input lines which are reserved for Wiegand communication cannot be used for any other purposes. The controller can operated with Wiegand readers also via MCX402-BRD and MCX102-BRD expanders.

Note: In case of electrically incompatible Wiegand readers it might be necessary to install MCI-7 interfaces.

LED indicators

MC16 controller is equipped with 8 LED indicators on it board. The function of each LED is explained in table 3.
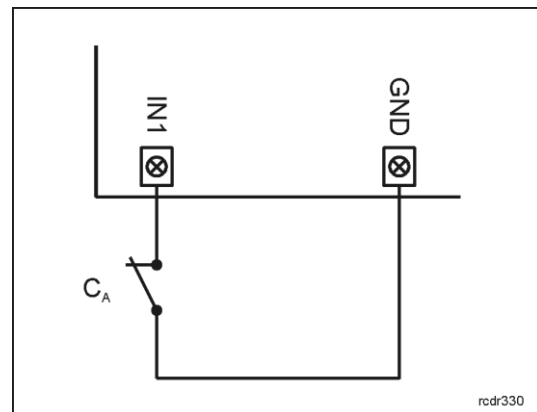
Inputs

The controller offers 8 general purpose NO and NC input types. These types and input response times are defined within low level configuration (RogerVDM or VISO v2). Functions are assigned to inputs within high level configuration (VISO).
The controller can monitor not only inputs on its board but also inputs located at peripheral devices (MCT, MCX). In case of MCX2D and MCX4D expanders it is possible define not only NO and NC types but also 3EOL/DW/NO and 3EOL/DW/NC types. The number of physical inputs can be doubled when 3EOL/DW type is configured.

Table 1. Input types
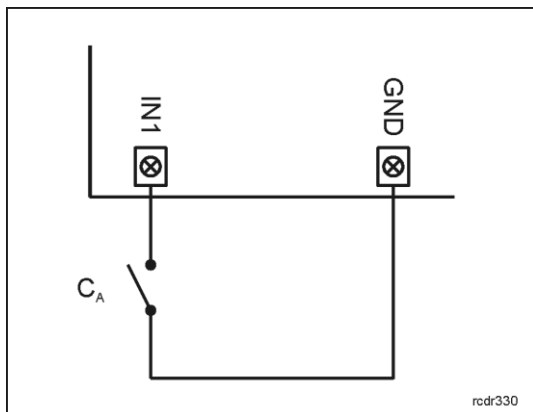
NO input	NC input
NO input can be in normal or in triggered state. In normal state C_A contacts are opened. Input triggering is caused by C_A contacts closing.	NC input can be in normal or in triggered state. In normal state C_A contacts are closed. Input triggering is caused by C_A contacts opening.

Response time

Response time parameter defines minimal impulse time on the input which triggers the input. Each input can be configured individually in range of 50 to 5000 ms within low level configuration (RogerVDM or VISO v2).

Outputs

The controller offers 6 transistor open collector type outputs (15V/150mA rated) and 2 relay outputs with NO/NC contacts (30V/1.5A DC/AC rated). Additionally 2 transistor outputs CLK and DTA are available if they are not used for RACS CLK/DTA interface. Electric parameters such as polarity are configured within low level configuration (RogerVDM or VISO v2). Function are assigned to outputs within high level configuration (VISO). Multiple functions with different priorities can be assigned to the same output at the same time.

The controller can activate not only outputs on its board but also outputs located at peripheral devices (MCT, MCX).

Memory card and license

The controller is equipped with FLASH memory card which among others offers event buffer (8 million) and it stores license file and configuration of the controller. Memory card and adequate license are necessary for controller functioning. If needed, the license.cfg file can be copied manually into memory card by means of memory card reader or in case of license upgrade it can be uploaded from VISO software by right clicking the controller and then selecting *Commands->Upload license file*.

In RACS 5 v2 system, in case of missing or incorrect license, the controller switches to service mode so then it is still possible to remotely upload correct license to the controller.
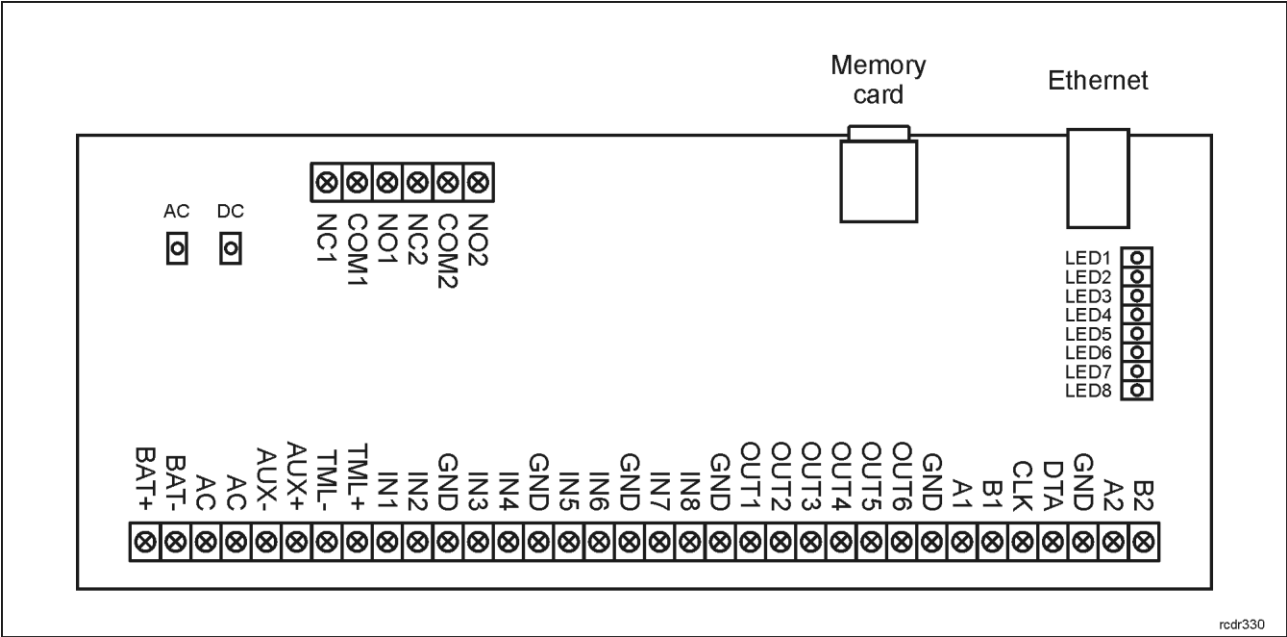
2. INSTALLATION

Fig. 2 MC16 controller board

Table 2. MC16 screw terminals	
Name	Description
BAT+, BAT-	Backup battery
AC, AC	18VAC or 24VDC input supply
AUX-, AUX+	12VDC/1,0A output supply (door lock)
TML-, TML+	12VDC/0,2A output supply (readers)
IN1-IN8	Inputs
GND	Ground
OUT1-OUT6	15VDC/150mA transistor output lines
A1,B1	RS485 bus
CLK, DTA	RACS CLK/DTA interface
A2,B2	Not used
NO1, COM1, NC1	30V/1,5A DC/AC relay (REL1)
NO2, COM2, NC2	30V/1,5A DC/AC relay (REL2)

Table 3. LED indicators	
Name	Description
LED1	Normal mode
LED2	ON: Service mode (low level configuration) Pulsing: RAM or Flash SPI memory error
LED3	ON: High level configuration error Pulsing: Low level configuration error
LED4	No card or memory card error

roger

LED5	Event log error
LED6	Not used*
LED7	Not used
LED8	Pulsing: Proper functioning

* In firmware 1.6.6 or older the LED6 was used to signal license error
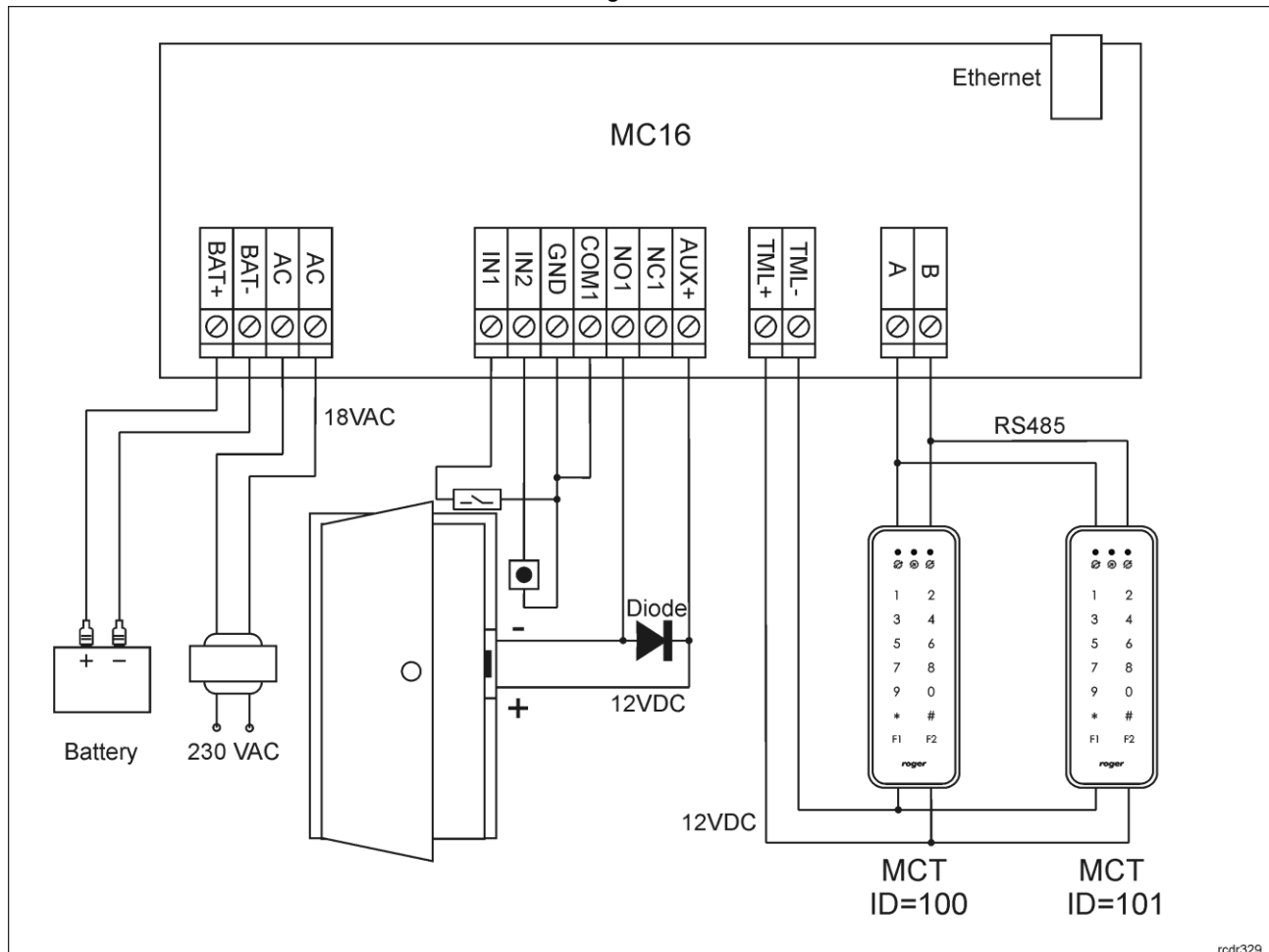

Fig. 3 Typical connection diagram for MC16-PAC-1 controller with MCT readers

Note: The simplest installation scenario with single door controller and MCT series readers is shown in fig. 3. Other installation scenarios are shown in AN002, AN029, AN030, AN031 and AN033 application notes and MC16-PAC-x-KIT installation manuals.

Installation guidelines

- Install device in such way as to ensure easy access to its screw terminals, sockets and memory card.
- All electrical connections must be done with disconnected power supply.
- All devices connected to the same communication bus (RS485 and RACS CLK/DTA) should be connected to the same negative potential (GND). Therefore all GND terminals from various power supply units used in the system should be connected with each other.
- Before the decision on using the device, it is recommended to carry out tests confirming the satisfactory quality of its operation in the target LAN / WAN network. This note does not apply to isolated LANs reserved exclusively for the access control system (or other system in which the device is to be used) in which the operation of the device is covered by the manufacturer's warranty. It should be assumed that a positive test result is not a guarantee of the correct operation of the

device or system because the conditions in the network can change significantly and/or be subject to cyber attacks.

3. LOW LEVEL CONFIGURATION AND RESET

Low level configuration (RogerVDM)

The purpose of low level configuration is to prepare device for operation in RACS 5 system. During initial low level configuration define own IP address and communication key. Programming of other parameters depends on the individual installation scenario requirements and is not obligatory.

Programming procedure with RogerVDM software (firmware 1.4.2 or newer)

1. Connect the controller to Ethernet network and define IP address of your computer with RogerVDM software in the same network as the controller with default IP address 192.168.0.213.
2. Start RogerVDM software, select *MC16 v1.x* device, firmware version and *Ethernet* communication channel.
3. Select from the list or enter manually the IP address of controller, enter 1234 communication key and establish connection with the controller.
4. In the top menu select *Tools* and *Set communication key* to define your own password for MC16 controller.
5. In *IP address* field define own address for the controller.
6. If the controller is supposed to operate with PRT series and/or Wiegand readers then activate them
7. Optionally enter comments for controller objects to facilitate their identification during further configuration of the system.
8. Optionally make a backup by clicking *Send to File…*
9. Click *Send to Device* to update the configuration of the controller an disconnect selecting *Device* in the top menu and then *Disconnect*.

Programming procedure with RogerVDM software (firmware 1.3.2 or older):

1. Connect the controller to Ethernet network and define IP address of your computer with RogerVDM software in the same network as the controller with default IP address 192.168.0.213.
2. Disconnect power supply.
3. Short CLK and DTA lines.
4. Restore power supply, all LED1-8 will flash and then wait min. 6s.
5. Remove connection between CLK and DTA lines (LEDs stop flashing, LED2 is ON).
6. Start RogerVDM software, select *MC16 v1.x* device, firmware version and *Ethernet* communication channel.
7. Enter the Service IP Address (it is specified in IP.INI file on the controller's memory card), enter the communication key (factory key is 1234) and establish connection with the controller.
8. In the top menu select *Tools* and *Set communication key* to define your own password for MC16 controller.
9. In *IP address* field define own address for the controller.
10. If the controller is supposed to operate with PRT series and/or Wiegand readers then activate them
11. Optionally enter comments for controller objects to facilitate their identification during further configuration of the system.
12. Optionally make a backup by clicking *Send to File…*
13. Click *Send to Device* to update the configuration of the controller an disconnect selecting *Device* in the top menu and then *Disconnect*.

Note: When low level configuration of controller is modified in working system, then additionally start VISO software detect again the controller, replace and synchronise settings. More information on migration to RACS 5 v2 system is given in AN015 application note.

Table 4. Low level configuration parameters	
Communication	
IP address	Device IP address.
Default gateway	Gateway IP address.

Subnet mask	Subnet mask.
RS485 answer timeout [ms]	Parameter defines maximal delay for peripheral device response on RS485 bus. Range: 25-500. Default value: 250.
RS485 encryption	Parameter enables encryption on RS485 bus. Range: [0]: No, [1]: Yes. Default value: [0]: No.
RS485 encryption key	Parameter defines key for encryption of communication at RS485 bus. Range: 4-16 ASCII characters.
RACS CLK/DTA readers	
Terminal 1 (RACS CLK/DTA ID0)	Parameter enables PRT series reader with ID=0 address. Range: [0]: OFF, [1]: ON. Default value: [0]: OFF.
Terminal 2 (RACS CLK/DTA ID1)	Parameter enables PRT series reader with ID=1 address. Range: [0]: OFF, [1]: ON. Default value: [0]: OFF.
Terminal 3 (RACS CLK/DTA ID2)	Parameter enables PRT series reader with ID=2 address. Range: [0]: OFF, [1]: ON. Default value: [0]: OFF.
Terminal 4 (RACS CLK/DTA ID3)	Parameter enables PRT series reader with ID=3 address. Range: [0]: OFF, [1]: ON. Default value: [0]: OFF.
Wiegand readers	
Terminal 5 (Wiegand 1)	Parameter enables Wiegand reader on IN1/IN2 inputs. Range: [0]: OFF, [1]: ON. Default value: [0]: OFF.
Terminal 6 (Wiegand 2)	Parameter enables Wiegand reader on IN3/IN4 inputs. Range: [0]: OFF, [1]: ON. Default value: [0]: OFF.
Terminal 7 (Wiegand 3)	Parameter enables Wiegand reader on IN5/IN6 inputs. Range: [0]: OFF, [1]: ON. Default value: [0]: OFF.
Terminal 8 (Wiegand 4)	Parameter enables Wiegand reader on IN7/IN8 inputs. Range: [0]: OFF, [1]: ON. Default value: [0]: OFF.
Wiegand format	Parameter defines data format from Wiegand readers. Range: [0]: Auto, [1]: Without control bits, [2]: Without extreme bits, [3]: With control bits. Default value: [0]: Auto.
Terminal settings	
Terminal 1-8: Type and class	Parameter defines type and class of authentication factor returned by terminal. Default value: 0x00100001.
Terminal 1-8: Keypad type	Parameter defines terminal keypad type. Range: [0]: OFF, [1]: Digits, [2]: Digits 2F, [3]: Digits 4F, [4]: PIN only. Default value: [4]: Only PIN.
Terminal 1-8: Keypad timeout	Parameter defines terminal keypad timeout. Range: 0-10000. Default value: 10000.
Input types	
IN1-IN8	Parameter defines type of input lines. Range: [1]: NO, [2]: NC, [9]: 3EOL/DW/NO, [10]: 3EOL/DW/NC. Default value: [1]: NO.
Input response times	
IN1-IN8 [ms]	Parameter defines minimal duration of pulse which is required to trigger the input. Range: 50-5000. Default value: 300.
Parametric (EOL) input resistances	
Tamper [Ohm]	Parameter defines Tamper resistor for parametric (EOL) inputs. Default value: 1k.
Alarm A [Ohm]	Parameter defines Alarm A resistor for parametric (EOL) inputs. Default value: 2.2k.

Alarm B [Ohm]	Parameter defines Alarm B resistor for parametric (EOL) inputs. Default value: 5.6k.
Output reversed polarity	
OUT-OUT6, REL1, REL2, CLK, DTA	Parameter defines default output status. Range: [0]: No, [1]: Yes. Default value: [0]: No.
Output functions	
OUT1-OUT6, REL1, REL2, CLK, DTA	Parameter defines output function which can be used to control Wiegand terminal.
Advanced settings	
Battery test period [s]	Parameter defines time between successive battery tests. Default value: 600
AC lost delay [s]	Parameter defines time after which lost AC supply is reported. Default value: 300.
Device comments	
DEV comment	Parameter defines any text or comment which corresponds to the device. It is later displayed in VISO program.
Configuration ID	Unique number which corresponds to current low level configuration of device.
Power supply comments	
PWR	Parameter defines any text or comment which corresponds to the object. It is later displayed in VISO program.
Terminal comments	
Terminal 1-8	Parameter defines any text or comment which corresponds to the object. It is later displayed in VISO program.
Input comments	
IN1-IN8	Parameter defines any text or comment which corresponds to the object. It is later displayed in VISO program.
Output comments	
OUT1-OUT6, REL1, REL2, CLK, DTA	Parameter defines any text or comment which corresponds to the object. It is later displayed in VISO program.

Low level configuration (VISO v2)

According to AN006 application note, in RACS 5 v2 system the low level configuration of already connected MC16 controller and its peripheral MCT/MCX devices can be done remotely from VISO v2 software.

Memory card settings

MC16 controller is equipped with FLASH memory card, where additional configuration files are stored. DEBUG.CFG test file on memory card enables additional diagnostics, communication control, etc. The configuration of the file is optional and useful in case of unusual problems with device functioning.

Table 5. DEBUG.CFG file parameters	
Parameter	Description
CON	Diagnostic console on the second RS485 bus of the controller is enabled when CON=1. Additionally the parameter DEL decides if full or selected data is transmitted and displayed. Range: 0 - 1. Default value: 0.
DEL	Full diagnostic data is stored in files on controller memory card and displayed on console

	when DEL=1. Range: 0 - 1. Default value: 0.
TWT	Diagnostic timer which restarts MC16 communication process when communication problems with Communication Server (RogerSVC) are detected. The parameter defines delay in minutes between problem detection and process restarting. When set to 0 then disabled. Range: 0 – 273. Default value: 3.
TRP	Periodic restarting of MC16 communication process. The parameter defines restarting frequency in minutes. When set to 0 then disabled. Range: $0 - 2^{24}$. Default value: 0.
CRT	Periodic restarting of MC16 controller at certain time every day. The format of parameter is hh.mm.
AGT	Gratuitous ARP (GARP) broadcasting in Ethernet network. The parameter defines broadcasting frequency in the unit of 10 s. When set to 0 then periodic broadcasting is disabled. Default value: 3 (i.e. 30s).
STD	Parameter of MC16-SVC controller.
EVL	Parameter of MC16-SVC controller.
DIP	DHCP is enabled when DIP=1. In such case the static IP address of controller is not applied. Range: 0 - 1. Default value: 0.
TAM	Two Users Mode with Thread Level verification is enabled when TAM=1. Range: 0 - 1. Default value: 0.
ETI, ETP	Parameters used in integration with DCS type elevator systems.

Memory reset

Memory reset erases all low level configuration settings including empty communication key and default 192.168.0.213 IP address of the controller. In case of firmware 1.3.2 or older the service IP address remains unchanged and is still kept in IP.INI file on the memory card.

Memory reset procedure:

1. Disconnect power supply.
2. Short CLK and IN4 lines.
3. Restore power supply, all LED1-8 will flash and then wait min. 6s.
4. Remove connection between CLK and IN4 lines (LEDs stop flashing, LED2 is ON).
5. Wait approx. 1.5 min till LED5+LED6+LED7+LED8 are flashing.
6. Restart the controller (switch power supply off and on)
7. Start low level configuration.

Note: In case of controller with firmware 1.4.2, make the first low level configuration as in case of controller with firmware 1.3.2.

Note: If the parameter DIP=1 is enabled in DEBUG.CFG file on the memory card of controller then DHCP will remain enabled after the reset.

Firmware update

New firmware can be uploaded to the controller using RogerVDM software or directly via memory card. Make a backup of low level configuration and save the settings to file as firmware update usually restores factory default settings and erases communication key. The file with the latest firmware is available at www.roger.pl.

Firmware update procedure (VISO v2)
In the top menu of VISO v2 software select *System->Update Firmware* or in the navigation tree of VISO v2 software right click Networks, Communication Server, Controller Group or particular controller and then select *Commands->Update Firmware*. In case of firmware update on the level of VISO v2 software it is possible to update firmware of many controllers at once.

Firmware update procedure (RogerVDM):

1. Establish connection with the controller using RogerVDM software.
2. Make a backup of low level configuration by clicking *Send to File…*
3. In the top menu select *Tools* and then *Update Firmware*.
4. Select firmware file and click *Update*.
5. After firmware upload wait till LED8 is flashing.
6. Start or restore low level configuration with RogerVDM.

Firmware update procedure (memory card):

1. Remove power supply.
2. Remove FLASH memory card from the controller.
3. Copy the new firmware to the memory card and rename it as *FW.BUF*.
4. Insert the memory card back again to the controller socket.
5. Power up the unit and wait till LED8 is flashing.
6. Start or restore low level configuration with RogerVDM software.

Note: During the firmware update process, it is necessary to ensure continuous and stable power supply for the MC16 module. The power supply failure may result in device repair by Roger service.

Note: When low level configuration of controller is modified in working system, then additionally start VISO software detect again the controller, replace and synchronise settings. More information on migration to RACS 5 v2 system is given in AN015 application note.

Note: When controller is downgraded from firmware newer than 1.6.6 to older version then it is necessary to configure the communication key by means of RogerVDM program.

4. HIGH LEVEL CONFIGURATION (VISO)

The high level configuration is conducted by means of VISO software and it is dedicated to define the logic of MC16 controller. It requires configuration of logic objects and their interrelations. Available MC16 objects and their parameters are listed below.

The configuration of exemplary RACS 5 system is explained in AN006 application note which is available at www.roger.pl

Main Board

Main Board is logic object which is created automatically when MC16 controller is enrolled into system and its hardware resources are detected. The Main Board represents MC16 module and it enables to define such objects as Inputs, Outputs, Function keys and Local Commands with functions dedicated to the Main Board. Tamper detectors for peripheral devices (MCT, MCX, PRT) are configured within the Main Board inputs.

Tab Inputs

The tab enables to define Input objects on the level of Main board. Parameter and functions are listed in the description of Input objects.

Tab Outputs

The tab enables to define Output objects on the level of Main board. Parameter and functions are listed in the description of Output objects.

Tab Function keys

The tab enables to define Function key objects on the level of Main board. Parameter and functions are listed in the description of Function key objects.

Tab Local commands

The tab enables to define Local commands objects on the level of Main board. Parameter and functions are listed in the description of Local commands objects.

Access Terminals

Access Terminals are logic objects representing physical devices which can be used for user identification and for starting action(s) by user. Each Access Terminal must be linked with physical reader, keypad, touchpanel or other device which enables certain actions. Access Terminals are assigned to Access Points.

Area General

Text box **Name** – enables to name the terminal.

Text box **Description** – enables to enter custom description of the terminal.

Area Object

Parameter **Object** – enables selection of physical reader (CDI object).

Info box **Device** – specifies reader model.

Info box **Name** – specifies type of object.

Info box **Comment** – displays comment which was assigned to the reader (DEV) during low level configuration.

Info box **IP Address** – specifies IP address of host device (controller) with connected reader.

Info box **RS Address** – specifies RS485 address of the reader.

Info box **Hardware version** – specifies hardware version of the reader.

Info box **Firmware version** – specifies firmware version of the reader.

Access Points

Access Point represents one or more equally treated Access Terminals. Access Point can be used for access granting at Access Door or for starting other actions in the system e.g. Alarm Zone arming/disarming, Time&Attendance registration, etc. Access Point can be a component of Access Zone as Entry, Exit or Internal Point. In such scenario it can be used among others for anti-passback, occupancy limits, and neighboring zones. Access Point does not have to be linked to Access Door and it can be used for identification of users for the purpose of Time&Attendance, building automation control, authentication before input (button) activation, etc. The identification of user at Access Point must be in accordance with Authentication Policy (e.g. Card and PIN, Only card, etc.)
Read in/out doors can be linked with two Access Points each with single Access Terminal or with single Access Point including two Access Terminals. In the first scenario Authorisations (access rights) can be defined separately for each direction while in the second case there is a single Authorisation for the door regardless of user movement direction.
Authentication Options, Inputs, Outputs, Function keys and Local commands can be defined within Access Point while Access Terminals and Access Doors can be assigned to Access Point. Based on Authentication Options the Access Point can recognize various method of card reading (single, double, long) and link them with various actions in the system.

Area General

Text box **Name** – enables to name the point.

Text box **LCD Message** – enables to specify point's name which will be used on display.

Parameter **Keypad Shortcut** – enables to select key which will correspond to the point when interactive options are applied.

Text box **Description** – enables to enter custom description for the point.

Tab Authentication

Parameter **Default Authentication Policy** – specifies default identification method for users at the point (e.g. card and PIN, Only card, etc.)

Parameter **Authentication Policy Schedule** – enables assignment of schedule to specify Authentication Policies for the Access Point in various periods. It requires earlier defining of Authentication Policy type Schedule.

Parameter **Failed Attempts Time [s]** – specifies the time when user identification attempts with unknown Authentication Factor are monitored for the purpose of Access Point blocking.

Parameter **Failed Attempts Limit** – specifies the number of user identification attempts with unknown Authentication Factor for the purpose of Access Point blocking.

Parameter **Failed Attempts Blocking Time [min]** – specifies the time for Access Point blocking when *Failed Attempt Limit* is reached within *Failed Attempt Time*. It is possible to block the point indefinitely and then the point can be unblocked with *[258]* input function.

Tab Access Modes

Parameter **Default Access Mode** – specifies how the access request from user at Access Point is processed in the system. More information on Access Modes is given in AN025 Application Note.

- **Normal Access** – access is granted after verification of user Authorisation (access right).
- **Positive Access** – access granting does not require user Authorisation (access right) so any user defined in the system can be granted access.
- **Negative Access** – access is denied regardless of user Authorisation (access right) excluding Access Credentials with Master exemption.
- **External Access** – access requires user Authorisation (access right) and additionally it must be approved with input function *[185]* or remotely on the level of VISO software.
- **Delayed Access** – access resulting from user Authorisation (access right) is delayed and then it can be denied with input function *[186]* or remotely on the level of VISO software.
- **Disabled Access** – access is denied regardless of user Authorisation (access right) including Access Credentials with Master exemption.

Parameter **External Access Time [s]** – specifies maximal time for accepting/denying access request in case of External Access Mode.

Parameter **Delayed Access Time [s]** – specifies maximal time for accepting/denying access request in case of Delayed Access Mode.

Tab Zone Options

Info box **Alarm Zone** – specifies Alarm Zone to which the Access Point is assigned to.

Info box **Entry Point** – specifies Access Zone for which the Access Point is Entry Point.

Info box **Exit Point** – specifies Access Zone for which the Access Point is Exit Point.

Info box **Internal Point** - specifies Access Zone for which the Access Point is Internal Point.

Option **Occupancy Count Enabled** – when the option is disabled then occupancy count and anti-passback are not applied at this Access Point. By default the option is enabled.

Option **Lower Limit Enabled** – when the option is disabled then access restrictions related to Occupancy Count Lower Limit are not applied. By default the option is enabled.

Option **Upper Limit Enabled** – when the option is disabled then access restrictions related to Occupancy Count Upper Limit are not applied. By default the option is enabled.

Tab T&A Options

Parameter **Default T&A Mode** – specifies default Time and Attendance Mode at the Access Point.

Parameter **T&A Mode Schedule** – enables assignment of schedule to specify T&A Modes for the Access Point in various periods. It requires earlier defining of Time and Attendance type Schedule.

Option **Register T&A Event when physical access is granted** – when the option is enabled then every access granting will additionally generate Time and Attendance event if a user is assigned with Advanced Authorisation for the function *[155]*. If the option *Zone entry/exit counted only after door opening* is enabled than T&A Event is registered when door opening signal from the input with function *[130]* is detected and not directly after access granting unless the Access Point is not associated with any Access Door.

Tab Advanced Options

Parameter **Thread Level** – specifies access level at the Access Point. If Thread Level of Access Credential belonging to particular user is lower than Thread Level of Access Point then access is denied regardless of Authorisation assigned to user's Access Credential.

Option **Cancel Door Open Too Long Alarm after access is granted** – when the option is enabled then controller cancels Door Open Too Long Alarm when access is granted at the door.

Option **Cancel Door Forced Alarm after access is granted** – when the option is enabled then controller cancels Door Forced Alarm when access is granted at the door.

Option **Zone entry/exit counted only after door opening** – when the option is enabled then user entry/exit into/from Access Zone is counted only if access granting is followed by actual door opening which is confirmed by door contact connected to controller input with the function *[130]*. The option concerns such Access Zone functionalities as anti-passback (APB), occupancy count and neighboring zones. Additionally it

affects the option *Register T&A Event when physical access is granted.* The option enables to apply TrueAPB.

Option *Zone entry/exit counted when door opened* – when the option is enabled then the option *Zone entry/exit counted only after door opening* is modified and then during door opening which is detected by means of door contact connected to controller input with the function *[130]*, multiple users who are granted access can be counted as entering/leaving particular Access Zone. In other words when the option is enabled then controller is not expecting that each user will complete full sequence individually (identification, access granting and door opening) as they can identify and be granted access during the same door opening.

Option *Two Users Mode* – when the option is enabled then access can be granted only if two Access Credentials with adequate Authorisations are used at the Access Point.

Option *Deny access on random personal check* – when the option is enabled then in case of randomly selected user not only output with the function *[89]* is activated but additionally access is denied at the Access Point.

Parameter *Access Direction* – specifies the direction of user movement when access is granted at the Access Point. The parameter is used mainly in turnstile control which is explained in AN019 application note. Available values:

- **None** – parameter disabled.
- **Read-in** – when access is granted at the Access Point then outputs with functions *[037]* and *[035]* are activated.
- **Read-out** – when access is granted at the Access Point then outputs with functions *[038]* and *[036]* are activated.
- **Read-in/out** – when access is granted at the Access Point then outputs with functions *[037], [038, [035]* and *[036]* are activated.

Parameter *Card Holder Location* – enables to indicate which Access Terminal of the Access Point is equipped with card holder so Authentication Options which require card holder could be used. Terminals with card holders (e.g. MCT82M-IO-CH) are mainly used in hotel application to control power supply in a room.

Parameter *Buzzer Signalization Priority* – specifies priority in range of 1-16 for BUZZER output control by terminal's internal logic. BUZZER output can be also assigned with output function(s) by system administrator and it is possible to define priority for such function(s). Therefore the parameter enables to decide if administrator defined logic or internal logic has priority in BUZZER control. The higher the number the higher the priority.

Tab Authentication Options

The tab is available when an Access Point is created and it enables to define parameters for Normal Authentication (single use of Authentication Factor), Special Authentication (long card reading), Double Authentication (double use of Authentication Factor) and for card inserting and removing from holder. Configuration parameters for each Authentication Option are the same.

Parameter *Action Type* – specifies action type for particular option. Available types are function and Local Command.

Parameter *Action* – specifies the function or Local Command which will be started by user for particular option.

Parameter *Parameter* – specifies a parameter for the function of action. As an example, for the function *[153]: Set Momentary T&A Mode* the parameter is particular T&A Mode. The parameter is not configured in this field when Local Command is applied.

Parameter *Object* – specifies target object for the function of action. The parameter is not configured in this field when Local Command is applied.

Option *Register Action Event* – when the option is enabled then every action starting will additionally generate associated event in the system.

Area Authorisation Options

Option *User authentication required* – when the option is enabled then users can start object function or Local Command without Authorisation(s) assigned. It is enough that such users are equipped with Authentication Factors which are enrolled in the system.

Option **Authorisation for Access Point required** – when the option is enabled then only users with proper Authorisation can start object function or Local Command. The Authorisation must include Access Point type Positive rule for the Access Point where the function is started.

Option **Authorisation for Object required** – when the option is enabled then only users with proper Authorisation can start object function or Local Command. The Authorisation must include Object type Positive rule for the object of the function.

Option **Authorisation for Function Parameter required** – when the option is enabled then users with proper Authorisation can start object function or Local Command. The Authorisation must include Parameter type Positive rule for the parameter of the function.

Area Interactive Options

Interactive options enable to start actions which are not defined within Authentication Options of an Access Point. Action can be started for any object depending on user Authorisations. Interactive actions can be started only on terminals with keypad. Such terminals must have the option *[*] key press allowed before PIN* enabled during their low level configuration (RogerVDM or VISO v2).

Option **Enable Function Selection** – when the option is enabled then user can enter keypad commands to start functions on the level of Alarm Zones *[102]-[104], [106]-[109]*, Access Doors *[121]-[127], [136]*, Access Points *[151]-[152], [159], [171]-[176]*, T&A Modes *[175]* and Access Modes *[178]-[186]*.

Option **Enable Object Selection** – when the option is enabled then user must enter object Keypad Shortcut to select the object.

Option **Enable Function Parameter Selection** – when the option is enabled then user must enter function parameter.

Tab Access Doors

The tab is available when an Access Point is created and it enables to assign Access Door to the point.

Tab Access Terminals

The tab is available when an Access Point is created and it enables to assign Access Terminal(s) to the point.

Tab Inputs

The tab is available when an Access Point is created and it enables to assign Input(s) to the point. Input parameters and functions are listed within the description of Input objects.

Tab Outputs

The tab is available when an Access Point is created and it enables to assign Output(s) to the point. Output parameters and functions are listed within the description of Output objects.

Tab Function Keys

The tab is available when an Access Point is created and it enables to assign Function Key(s) to the point. Function key parameters and functions are listed within the description of Function Key objects.

Tab Local Commands

The tab is available when an Access Point is created and it enables to assign Local Command(s) to the point. Local Command parameters and functions are listed within the description of Local Command objects.

Access Doors

Access Door represents physical door or gate with such devices as door lock, exit button, door contact, etc. Access Doors are logically linked with Access Points.

Area General

Text box **Name** – enables to name the door.

Parameter **Group** – enables to assign door to previously created Access Door Group.

Text box **LCD Message** – enables to specify door's name which will be used on display.

Parameter **Keypad Shortcut** – enables to select key which will correspond to the door when interactive options are applied.

Text box **Description** – enables to enter custom description for the door.

Area Door Mode Options

Parameter *Default Door Mode* – specifies default Door Mode. Available values:

- *Normal* – access can be granted for user with adequate Authorisation(s).
- *Unlocked* – access is granted without user identification. Door lock is permanently released.
- *Conditional Unlocked* – the door is in Normal Mode and when access is granted based on user Authorisation(s), then it switches to Unlocked Mode.
- *Locked* – access cannot be granted regardless of user Authorisation(s). Door lock is permanently locked.

Parameter *Door Mode Schedule* – enables assignment of schedule to specify Door Modes for the Access Door in various periods. It requires earlier defining of Door Mode type Schedule.

Area Door Options

Parameter *Re-lock* – specifies if door lock release is shortened after access granting. Available values:

- *Disabled* – parameter disabled.
- *Clear lock pulse after door opening* – the output for door lock control is released after door opening detection i.e. after signal from input with the function *[130]* (door contact) and not after time defined by the parameter *Lock Pulse* or *Lock Pulse Extended*.
- *Clear lock pulse after door closing* – the output for door lock control is released after door closing detection i.e. after signal from input with the function *[130]* (door contact) and not after time defined by the parameter *Lock Pulse* or *Lock Pulse Extended*.

Parameter *Lock Pulse [s]* – specifies default door lock release time when access is granted based on input functions *[128]*, *[151]* or *[175]*.

Parameter *Lock Pulse Extended [s]* – specifies default door lock release time when access is granted based on input functions *[129]*, *[152]* or *[176]*.

Parameter *Lock Pulse Delay [s]* – specifies delay for door lock release when access is granted.

Parameter *Door Open Too Long Time [s]* – specifies maximal time to close the door. When elapsed then Door Open Too Long Alarm is raised.

Option *Cancel Door Open Too Long Alarm when door closed* – when the option is enabled then door closing cancels Door Open Too Long Alarm.

Option *Door Open Too Long Alarm not only in Normal Door Mode* – when the option is enabled then Door Open Too Long Alarm can be raised also for other than Normal Door Modes.

Parameter *Door Open Too Long Prealarm Time [s]* – specifies when the prealarm (output with function *[030]*) is activated to warn that Door Open Too Long Alarm will be raised soon. The parameter defines how many seconds before the alarm, the warning (prealarm) is started.

Option *Disable event [321]: Door Forced Alarm* – when the option is enabled then event *[321]* is not generated for the Access Door.

Tab Inputs

The tab is available when an Access Door is created and it enables to assign Input(s) to the door. Input parameters and functions are listed within the description of Input objects.

Tab Outputs

The tab is available when an Access Door is created and it enables to assign Output(s) to the door. Output parameters and functions are listed within the description of Output objects.

Tab Function Keys

The tab is available when an Access Door is created and it enables to assign Function Key(s) to the door. Function key parameters and functions are listed within the description of Function key objects.

Tab Local Commands

The tab is available when an Access Door is created and it enables to assign Local Command(s) to the door. Local Command parameters and functions are listed within the description of Local Command objects.

Inputs

Input represents object dedicated to receiving electric signals from external device/system. The status of input is monitored and when changed then action can be started by controller. Type of action depends on the function assigned to particular input (e.g. door opening detection, T&A Mode selection, arming, etc.)

One or more functions can be assigned to single input. When multifunction input is applied then its triggering may start multiple actions in the system. More information on multifunction lines is given in AN010 application note. In case of inputs with the same toggle functions within the same object it is possible to apply AND/OR logic. Additionally, in order to trigger an input in the system it may be necessary to authenticate user at selected Authentication Point (reader).

Area General

Text box *Name* – enables to name the input.

Text box *LCD Message* – enables to specify input's name which will be used on display.

Parameter *Keypad Shortcut* – enables to select key which will correspond to the input when interactive options are applied.

Text box *Description* – enables to enter custom description for the input.

Area Object

Parameter *Name* – enables selection of physical input.

Info box *Device* – specifies device with selected input.

Info box *Label* – specifies type of object.

Info box *Comment* – displays comment which was assigned to the input during low level configuration.

Info box *Type* – specifies type of input (e.g. NO).

Info box *IP Address* – specifies IP address of host device (controller).

Info box *RS Address* – specifies RS485 address of device with the input.

Area Additional Options

Parameter *Activity Schedule* – enables assignment of schedule to specify when input can be triggered. It requires earlier defining of General Purpose Maintained type Schedule.

Parameter *Authentication Point* – specifies Access Point where user must authenticate before input is triggered. Such authentication requirement is configured in the area *Authorisation Options* when input is assigned to particular object (e.g. Access Door).

Option *Multifunction* – when the option is enabled then it is possible to specify the maximal number functions for assignment to the input.

Parameter *Function Limit* – specifies the maximal number of functions for assignment to the input.

Area Events

Option *Register event when input is switched ON* – when the option is enabled then input triggering will generate an event in the system.

Parameter *Input ON Event* – enables to indicate what event is generated in the system when the input is triggered. It could be default event *[661]* or any other administrator defined event.

Option *Register event when input is switched OFF* – when the option is enabled then input releasing will generate an event in the system.

Parameter *Input OFF Event* – enables to indicate what event is generated in the system when the input is released. It could be default event *[662]* or any other administrator defined event.

Input object can be further configured, mainly in regard of its function on the level of other objects e.g. Access Door. Other parameters for such configuration are given below, while parameters specific for particular function are explained in the description of such function in the table 6.

Area General

Parameter *Input* – enables to select Input object.

Parameter *Function* – enables to select function for the Input. The list of all available functions is given in the table 6 below.

Parameter *Parameter* – specifies parameter of selected function. It is available for some functions only.

Option *Register Action Event* – when the option is enabled then input triggering generates event related to input function.

Parameter *Logic Function* – specifies logic function for the input. Available values:

- *OR* – default value. Target object of the function is activated when at least single input with the function is triggered.

- *I* – value is available only for toggle type inputs. Target object is activated when all inputs with the function are triggered.

Area Authorisation Options

Option *User authentication required* – when the option is enabled then users can trigger the input without Authorisation(s) assigned. It is enough that such users are equipped with Authentication Factors which are enrolled in the system.

Option *Authorisation for Access Point required* – when the option is enabled then only users with proper Authorisation can trigger the input. The Authorisation must include Access Point type Positive rule for the Access Point where the function is started.

Option *Authorisation for Object required* – when the option is enabled then only users with proper Authorisation can trigger the input. The Authorisation must include Object type Positive rule for the object of the function.

Option *Authorisation for Function Parameter required* – when the option is enabled then users with proper Authorisation can trigger the input. The Authorisation must include Parameter type Positive rule for the parameter of the function.

Input functions

Input functions are available within selected objects. For example, input line can be used for arming/disarming and then it should be configured on the level of Alarm Zone. Some of input functions can be used in Authentication Options on the level of Access Point.

Input functions are divided into event type which are triggered by pulse and toggle (status) type which are monitored in regard of their triggering and releasing.

Table 6 Input functions				
No.	Name	Type	Object	Description
060	Restart Controller without Dynamic Data Reload	Event	Main Board	When triggered then controller is restarted and all dynamic data (usage limits, occupancy limits, APB register, etc.) is deleted.
101	Armed ON Mode Toggle	Toggle	Alarm Zone	As long as triggered then alarm zone is maintained armed.
102	Set Alternately Armed ON/Armed OFF Mode	Event	Alarm Zone	When triggered then alarm zone is switched to opposite armed mode.
103	Set Armed ON Mode	Event	Alarm Zone	When triggered then Alarm Zone is armed.
104	Set Armed OFF Mode	Event	Alarm Zone	When triggered then Alarm Zone is disarmed.
105	Disable Armed ON Mode Toggle	Toggle	Alarm Zone	As long as triggered then Alarm Zone arming is blocked.
106	Postpone Auto-arming	Event	Alarm Zone	When triggered then Alarm Zone arming is delayed by the parameter *Auto-arming Delay when Zone not Ready for Arming*.
107	Request Armed ON Mode	Event	Alarm Zone	When triggered then outputs with functions *[045]* and *[047]* are activated. The function is also used to arm Integra or Galaxy alarm panel if it is integrated with RACS 5 system.
108	Request Armed OFF Mode	Event	Alarm Zone	When triggered then outputs with functions *[046]* and *[047]* are activated. The function is also used to disarm Integra or Galaxy alarm panel if it is integrated with RACS 5 system.
109	Request Alternately Armed ON/Armed OFF Mode	Event	Alarm Zone	When triggered then outputs with functions *[047]* and *[045]* or *[046]* depending on current mode are activated. The function is also used to arm/disarm Integra or Galaxy alarm panel if it is integrated with RACS 5 system.
111	Clear Occupancy Register	Event	Access Zone	When triggered then list of Access Credentials (and their users) registered in the zone is deleted. It affects mainly occupancy count in the zone.
112	Clear Anti-passback Register	Event	Access Zone	When triggered then APB register is deleted.
113	Restart Controller with Dynamic Data Reload	Event	Main Board	When triggered then controller is restarted and all dynamic data (usage limits, occupancy limits, APB register, etc.) is preserved.
114	TML Supply Output Overload Toggle	Toggle	Power Supply	As long as triggered then TML output overload is reported to controller.
115	AUX Supply Output Overload Toggle	Toggle	Power Supply	As long as triggered then AUX output overload is reported to controller.

116	AC Lost Toggle	Toggle	Power Supply	As long as triggered then lack of AC power supply is reported to controller.
117	Delayed AC Lost Toggle	Toggle	Power Supply	As long as triggered then delayed lack of AC power supply is reported to controller.
118	Low Battery Toggle	Toggle	Power Supply	As long as triggered then low battery charging level is reported to controller.
119	Battery Failure Toggle	Toggle	Power Supply	As long as triggered then battery failure is reported to controller.
120	Power Supply Overload Toggle	Toggle	Power Supply	As long as triggered then overload of power supply unit is reported to controller.
121	Set Emergency Door Unlocked Mode	Event	Access Door	When triggered then Access Door is switched to Emergency Unlocked Door Mode. Emergency type mode has higher priority than normal type mode which can be set with functions *[124] - [127]*. The function can be used in emergency door opening by fire alarm system.
122	Set Emergency Door Locked Mode	Event	Access Door	When triggered then Access Door is switched to Emergency Locked Door Mode. Emergency type mode have higher priority than normal type mode which can be set with functions *[124] - [127]*.
123	Clear Emergency Door Mode	Event	Access Door	When triggered then Emergency Door Mode is cleared and Normal Door Mode is restored.
124	Set Locked Door Mode	Event	Access Door	When triggered then Locked Door Mode at Access Door is set.
125	Set Unlocked Door Mode	Event	Access Door	When triggered then Unlocked Door Mode at Access Door is set.
126	Set Normal Door Mode	Event	Access Door	When triggered then Normal Door Mode at Access Door is set.
127	Set Conditional Unlocked Door Mode	Event	Access Door	When triggered then Conditional Unlocked Door Mode at Access Door is set.
128	Generate Door Lock Pulse	Event	Access Door	When triggered then door is opened for the time specified by the parameter *Lock Pulse* if it is in Normal Door Mode. Input with the function is used mainly for connection of exit button.
129	Generate Extended Door Lock Pulse	Event	Access Door	When triggered then door is opened for the time specified by the parameter *Lock Pulse Extended* if it is in Normal Door Mode.
130	Door Contact Toggle	Toggle	Access Door	As long as triggered then door opening is reported to controller. Input with the function is used for connection of door contact.
131	Access Door Bell	Event	Access Door	When triggered then bell is activated at Access Door and output with the function *[34]* is triggered.
132	Disable Door Toggle	Toggle	Access Door	As long as triggered then Access Door is blocked.

133	Tamper Toggle	Toggle	Main Board	As long as triggered then sabotage alarm (controller or terminal enclosure tampering) is raised and can be signalled by outputs with functions *[58]* and *[59]*.
134	Clear Door Forced Alarm	Event	Access Door	When triggered then Forced Door Alarm is cancelled.
135	Clear Door Open Too Long Alarm	Event	Access Door	When triggered then Door Open Too Long Alarm is cancelled.
136	Set Alternately Normal/Unlocked Door Mode	Event	Access Door	When triggered then Access door is switched between Normal and Unlocked Door Modes.
137	Emergency Unlocked Door Mode Toggle	Toggle	Access Door	As long as triggered then Access Door is switched to Emergency Unlocked Door Mode. Emergency type mode has higher priority than normal type mode which can be set with functions *[124] - [127]*. The function can be used in emergency door opening by fire alarm system.
138	Emergency Locked Door Mode Toggle	Toggle	Access Door	As long as triggered then Access Door is switched to Emergency Locked Door Mode. Emergency type mode has higher priority than normal type mode which can be set with functions *[124] - [127]*.
145	Set Node ON with Multiple Parametric Times	Event	Automation Node	When triggered then Automation Node is switched on for the time specified by function parameter *Parametric Time* with delay specified by node parameter *Default delay*. Series of input triggerings are added and consequently the Automation Node can be switched on for multiple parametric times.
146	Set Node ON with Multiple Default Times	Event	Automation Node	When triggered then Automation Node is switched on for the time specified by node parameter *Default Time* with delay specified by node parameter *Default delay*. Series of input triggerings are added and consequently the Automation Node can be switched on for multiple default times. *Total Time Limit* can be defined for the function to limit the maximal series of multiple default times.
147	Set Node OFF Toggle	Toggle	Automation Node	As long as triggered then Automation Node remains switched off.
148	Set Check-in Flag ON	Event	Access Point	When triggered then Check-in flag and outputs with functions *[240]*, *[242]* and *[243]* are switched on. The function is available only for MC16-HRC controllers.
149	Set Check-in Flag OFF	Event	Access Point	When triggered then Check-in flag and output with function *[243]* are switched off while outputs with functions *[241] and [242]* are switched on. The function is available only for MC16-HRC controllers.
150	Set Alternately Check-in Flag	Event	Access Point	When triggered then Check-in flag is switched to opposite state. Outputs with functions *[240], [241], [242]* and *[243]* are switched accordingly. The function

	ON/OFF			is available only for MC16-HRC controllers.
151	Grant Door Access with Normal Lock Pulse (detailed)	Event	Access Point	When triggered then Access Door of the Access Point is opened for the time specified by the parameter *Lock Pulse*. The function is usually used within *Authentication Options* of the Access Point but it can also be assigned to input. In the second case it is necessary to define *Authentication Point* and enable at least single option in the area *Authorisation Options*. Contrary to function *[175]* when this function is used then separate event is generated for each associated objects.
152	Grant Door Access with Extended Lock Pulse (detailed)	Event	Access Point	When triggered then Access Door of the Access Point is opened for the time specified by the parameter *Lock Pulse Extended*. The function is usually used within *Authentication Options* of the Access Point but it can also be assigned to input. In the second case it is necessary to define *Authentication Point* and enable at least single option in the area *Authorisation Options*. Contrary to function *[176]* when this function is used then separate event is generated for each associated objects.
153	Set Momentary T&A Mode	Event	Access Point	When triggered then Time&Attendance Mode is temporary selected at Access Point. After user identification or when 8 s elapses, the default T&A Mode is restored. Function parameter defines which T&A Mode is applied when input is triggered.
154	Set Maintained T&A Mode	Event	Access Point	When triggered then Time&Attendance Mode is permanently selected at Access Point. Function parameter defines which T&A Mode is applied when input is triggered.
155	Register T&A Event	Event	Access Point	When triggered and followed by user identification then Time&Attendance event is registered in the system. Function parameter defines which T&A Mode is applied when input is triggered.
156	Set Authentication Policy	Event	Access Point	When triggered then Authentication Policy is selected at Access Point. Function parameter defines which policy (e.g. Card and PIN) is applied when input is triggered.
157	Call Elevator	Event	Access Point	When triggered then elevator is called. The function is available only for MC16-EVK controllers and it is removed in RACS 5 v2 system.
158	Disable Door Access Toggle	Toggle	Access Point	As long as triggered then access granting at Access Point is disabled for all users including Access Credentials with Master exemption.
159	Access Point Bell	Event	Access Point	When triggered then bell is activated at Access Point and output with the function *[64]* is triggered.
161	Set Node ON Instantly	Event	Automation	When triggered then Automation Node is switched on without delay and

			Node	indefinitely i.e. *Default Time* and *Default Delay* parameters of the node are skipped.
162	Set Node ON with Default Time Settings	Event	Automation Node	When triggered then Automation Node is switched on according to *Default Time* and *Default Delay* parameters of the node. The function is affected by the option *Activation Extending*.
163	Set Node OFF Instantly	Event	Automation Node	When triggered then Automation Node is switched off without any delay.
164	Set Alternately Node ON/OFF Instantly	Event	Automation Node	When triggered then Automation Node is switched to opposite state without delay and indefinitely i.e. *Default Time* and *Default Delay* parameters of the node are skipped.
165	Set Alternately Node ON/OFF with Default Time Settings	Event	Automation Node	When triggered then Automation Node is switched to opposite state according to *Default Time* and *Default Delay* parameters of the node.
166	Set Node ON Toggle	Toggle	Automation Node	As long as triggered then Automation Node remains switched on.
167	Set Node ON with Parametric Time Settings	Event	Automation Node	When triggered then Automation Node is switched on according to *Parametric Time* and *Parametric Delay* parameters of the function. The function is affected by the option *Activation Extending*.
168	Set Node OFF with Parametric Time Settings	Event	Automation Node	When triggered then Automation Node is switched off according to *Parametric Delay* parameter of the function.
171	Register Guard Tour Event	Event	Access Point	When triggered then the event Guard Tour is recorded in the system and output with the function *[76]* is activated.
172	Register Trace Event	Event	Access Point	When triggered then the event Trace is recorded in the system and output with the function *[77]* is activated.
173	Register Muster Event	Event	Access Point	When triggered then the event Muster is recorded in the system and output with the function *[78]* is activated.
174	Register Duress Event	Event	Access Point	When triggered then the event Duress is recorded in the system and output with the function *[79]* is activated.
175	Grant Door Access with Normal Lock Pulse	Event	Access Point	When triggered then Access Door of the Access Point is opened for the time specified by the parameter *Lock Pulse*. The function is usually used within *Authentication Options* of the Access Point but it can also be assigned to input. In the second case it is necessary to define *Authentication Point* and enable at least single option in the area *Authorisation Options*. Contrary to function *[151]* when this function is used then single event is generated for all associated objects. The function is mainly used in case of elevators (MC16-

				EVC) and wired lockers (MC16-LCK).
176	Grant Door Access with Extended Lock Pulse	Event	Access Point	When triggered then Access Door of the Access Point is opened for the time specified by the parameter *Lock Pulse Extended*. The function is usually used within *Authentication Options* of the Access Point but it can also be assigned to input. In the second case it is necessary to define *Authentication Point* and enable at least single option in the area *Authorisation Options*. Contrary to function *[152]* when this function is used then single event is generated for all associated objects.
177	Set Access Mode	Event	Access Point	When triggered then Access Mode is selected at Access Point. Function parameter defines which mode is applied when input is triggered.
178	Set Default Access Mode	Event	Access Point	When triggered then Default Access Mode is selected at Access Point.
179	Set Negative Access Mode	Event	Access Point	When triggered then Negative Access Mode is selected at Access Point.
180	Set Positive Access Mode	Event	Access Point	When triggered then Positive Access Mode is selected at Access Point.
181	Set Normal Access Mode	Event	Access Point	When triggered then Normal Access Mode is selected at Access Point.
182	Set External Access Mode	Event	Access Point	When triggered then External Access Mode is selected at Access Point.
183	Set Delayed Access Mode	Event	Access Point	When triggered then Delayed Access Mode is selected at Access Point.
184	Set Disabled Access Mode	Event	Access Point	When triggered then Disabled Access Mode is selected at Access Point.
185	Grant Access for External Access Mode	Event	Access Point	When triggered then access is granted for External Access Mode. The function also affects Delayed Access Mode.
186	Deny Access for Delayed Access Mode	Event	Access Point	When triggered then access is denied for Delayed Access Mode. The function also affects External Access Mode.
187	Set Do Not Disturb Flag ON	Event	Access Point	When triggered then Do Not Disturb flag and outputs with functions *[224]*, *[226]* and *[227]* are switched on. The function is available only for MC16-HRC controllers.
188	Set Do Not Disturb Flag OFF	Event	Access Point	When triggered then Do Not Disturb flag and output with function *[227]* are switched off while outputs with functions *[225] and [226]* are switched on. The function is available only for MC16-HRC controllers.
189	Set Alternately Do Not Disturb Flag ON/OFF	Event	Access Point	When triggered then Do Not Disturb flag is switched to opposite state. Outputs with functions *[224], [225], [226]* and *[227]* are switched accordingly. The function is available only for MC16-HRC controllers.
190	Set Call Assistance Flag ON	Event	Access Point	When triggered then Call Assistance flag and outputs with functions *[228], [230]* and *[231]* are switched on. The function is available only for MC16-HRC

roger

				controllers.
191	Set Call Assistance Flag OFF	Event	Access Point	When triggered then Call Assistance flag and output with function *[231]* are switched off while outputs with functions *[229] and [230]* are switched on. The function is available only for MC16-HRC controllers.
192	Set Alternately Call Assistance Flag ON/OFF	Event	Access Point	When triggered then Call Assistance flag is switched to opposite state. Outputs with functions *[228], [229], [230]* and *[231]* are switched accordingly. The function is available only for MC16-HRC controllers.
193	Set Make Up Room Flag ON	Event	Access Point	When triggered then Make Up Room flag and outputs with functions *[232], [234]* and *[235]* are switched on. The function is available only for MC16-HRC controllers.
194	Set Make Up Room Flag OFF	Event	Access Point	When triggered then Make Up Room flag and output with function *[235]* are switched off while outputs with functions *[233] and [234]* are switched on. The function is available only for MC16-HRC controllers.
195	Set Alternately Make Up Room Flag ON/OFF	Event	Access Point	When triggered then Make Up Room flag is switched to opposite state. Outputs with functions *[232], [233], [234]* and *[235]* are switched accordingly. The function is available only for MC16-HRC controllers.
196	Set Service Flag ON	Event	Access Point	When triggered then Service flag and outputs with functions *[236], [238]* and *[239]* are switched on. The function is available only for MC16-HRC controllers.
197	Set Service Flag OFF	Event	Access Point	When triggered then Service flag and output with function *[239]* are switched off while outputs with functions *[237] and [238]* are switched on. The function is available only for MC16-HRC controllers.
198	Set Alternately Service Flag ON/OFF	Event	Access Point	When triggered then Service flag is switched to opposite state. Outputs with functions *[236], [237], [238]* and *[239]* are switched accordingly. The function is available only for MC16-HRC controllers.
199	Set Two Users Mode Toggle	Toggle	Access Point	As long as triggered then Two Users Mode is enabled at Access Point. In Two Users Mode the access can be granted only if two Access Credentials with adequate Authorisations are used at the Access Point.
204	Set Two Users Mode ON	Event	Access Point	When triggered then Two Users Mode is enabled at Access Point.
205	Set Two Users Mode OFF	Event	Access Point	When triggered then Two Users Mode is disabled at Access Point.
206	Set Cafeteria Flag ON	Event	Access Point	When triggered then Cafeteria flag and outputs with functions *[212], [214]* and *[215]* are switched on. The function is available only for MC16-HRC controllers.

roger

207	Set Cafeteria Flag OFF	Event	Access Point	When triggered then Cafeteria flag and output with function *[215]* are switched off while outputs with functions *[213] and [214]* are switched on. The function is available only for MC16-HRC controllers.
208	Set Alternately Cafeteria Flag ON/OFF	Event	Access Point	When triggered then Cafeteria flag is switched to opposite state. Outputs with functions *[212], [213], [214]* and *[215]* are switched accordingly. The function is available only for MC16-HRC controllers.
209	Set Luggage Service Flag ON	Event	Access Point	When triggered then Cafeteria flag and outputs with functions *[216], [218]* and *[219]* are switched on. The function is available only for MC16-HRC controllers.
210	Set Luggage Service Flag OFF	Event	Access Point	When triggered then Luggage Service flag and output with function *[219]* are switched off while outputs with functions *[217] and [218]* are switched on. The function is available only for MC16-HRC controllers.
211	Set Alternately Luggage Service Flag ON/OFF	Event	Access Point	When triggered then Luggage Service flag is switched to opposite state. Outputs with functions *[216], [217], [218]* and *[219]* are switched accordingly. The function is available only for MC16-HRC controllers.
220	Intruder Detection	Toggle	Alarm Zone	When triggered then intruder alarm is raised according to Alarm Zone settings in *Alarm Functions* area. The line can be used for connection of alarm detector.
221	Delayed Intruder Detection	Toggle	Alarm Zone	When triggered then delayed intruder alarm is raised according to Alarm Zone settings in *Alarm Functions* area. The line can be used for connection of alarm detector.
257	Disable Access Point	Event	Access Point	When triggered then identification at Access Point is disabled for all users including Access Credentials with Master exemption.
258	Enable Access Point	Event	Access Point	When triggered then Access Point is enabled if previously disabled with the function *[257]* or as a result of failed authentication attempts.
259	Disable Access Point Toggle	Toggle	Access Point	As long as triggered then access granting at Access Point is disabled for all users including Access Credentials with Master exemption.
260	Temporarily Increase Occupancy Upper Limit in Zone by 1	Event	Access Zone	When triggered then Occupancy Upper Limit in Access Zone is temporary increased by one. The function is available only for MC16-AZC controllers.
261	Temporarily Decrease Occupancy Upper Limit in Zone by 1	Event	Access Zone	When triggered then Occupancy Upper Limit in Access Zone is temporary decreased by one. The function is available only for MC16-AZC controllers.
262	Clear Temporary Modifications of Occupancy Upper Limit in Zone	Event	Access Zone	When triggered then all temporary modifications of Occupancy Upper Limit in Access Zone are cleared and primary limit is restored. The function is available only for MC16-AZC controllers.

263	Temporarily Increase Occupancy Upper Limit in Zone by Specified Number	Event	Access Zone	When triggered then Occupancy Upper Limit in Access Zone is temporary increased by value which is specified as function parameter. The function is available only for MC16-AZC controllers.
264	Temporarily Decrease Occupancy Upper Limit in Zone by Specified Number	Event	Access Zone	When triggered then Occupancy Upper Limit in Access Zone is temporary decreased by value which is specified as function parameter. The function is available only for MC16-AZC controllers.
269	Activate Personal Check	Event	Access Point	When triggered then personal check is started and output function *[89]* is activated for the next access granting. The function is operational only if random personal check is enabled at the Access Point i.e. output with the function *[89]* is configured. Therefore the purpose of function *[269]* is to manually affect random personal check.
270	Disable Thread Levels for Two Users Mode	Event	Access Point	When triggered then Thread Level is not verified at Access Point for Two Users Mode.
271	Enable Thread Levels for Two Users Mode	Event	Access Point	When triggered then Thread Level is verified at Access Point for Two Users Mode.
272	Set Alternately Thread Levels for Two Users Mode	Event	Access Point	When triggered then Thread Level verification is alternately switched on/off for Two Users Mode.
273	Thread Levels for Two Users Mode Toggle	Toggle	Access Point	As long as triggered then Thread Level is not verified at Access Point for Two Users Mode. When released then Thread level is verified.

Function Keys

Function Key represents additional, non-numeric key (F1, F2, F3, F4, *, #) which is available on keypad of some of MCT series readers, PRT series readers and other dedicated terminals. The status of key is monitored and when changed then action can be started by controller. Type of action depends on the function assigned to particular key (e.g. T&A Mode selection, arming, etc.) One or more functions can be assigned to single key. When multifunction key is applied then its triggering may start multiple actions in the system. More information on multifunction lines is given in AN010 application note. The controller can recognize normal and long key pressing and each can be assigned with individual function (short and long pressing requires additional low level configuration of the terminal). Additionally, in order to use a key in the system it may be necessary to authenticate user at selected Authentication Point (reader).

Area General

Text box *Name* – enables to name the key.

Text box *Description* – enables to enter custom description for the key.

Area Object

Parameter *Name* – enables selection of device with keypad (KBD object).

Parameter *Key Code* – enables selection of physical key on keypad.

Info box *Device* – specifies device with selected key.

Info box *Label* – specifies type of object.

Info box *Comment* – displays comment which was assigned to the keypad during low level configuration.

Info box *Type* – specifies type of keypad.

Info box *IP Address* – specifies IP address of host device (controller).

Info box *RS Address* – specifies RS485 address of device with the key.

Area Additional Options

Parameter *Activity Schedule* – enables assignment of schedule to specify when key can be used. It requires earlier defining of General Purpose Maintained type Schedule.

Parameter *Authentication Point* – specifies Access Point where user must authenticate before the key is used. Such authentication requirement is configured in the area *Authorisation Options* when the key is assigned to particular object (e.g. Access Door).

Option *Multifunction* – when the option is enabled then it is possible to specify the maximal number functions for assignment to the key.

Parameter *Function Limit* – specifies the maximal number of functions for assignment to the key.

Parameter *Key Press Type* – specifies key pressing method. By default normal pressing is available. Long pressing requires additional low level configuration of the terminal. Available values:

- *Short Press* – key pressing for less than 2 s (by default).
- *Long Press* – key pressing for more than 2 s (by default).

Area Events

Option *Register event when key is used* – when the option is enabled then key pressing will generate an event in the system.

Parameter *Function Key Event* – enables to indicate what event is generated in the system when the key is used. It could be default event *[660]* or any other administrator defined event.

Option *Register event when input is switched OFF* – when the option is enabled then input releasing will

Function Key object can be further configured, mainly in regard of its function on the level of other objects e.g. Access Door. Other parameters for such configuration are given below, while parameters specific for particular function are explained in the description of such function in the table 6.

Area General

Parameter *Function Key* – enables to select Function Key object.

Parameter *Function* – enables to select function for the key. The list of all available functions is given in the table 6 below.

Parameter *Parameter* – specifies parameter of selected function. It is available for some functions only.

Option **Register Action Event** – when the option is enabled then key pressing generates event related to key function.

Parameter **Logic Function** – not used for Function Key.

Area Authorisation Options

Option **User authentication required** – when the option is enabled then users can use the key without Authorisation(s) assigned. It is enough that such users are equipped with Authentication Factors which are enrolled in the system.

Option **Authorisation for Access Point required** – when the option is enabled then only users with proper Authorisation can use the key. The Authorisation must include Access Point type Positive rule for the Access Point where the function is started.

Option **Authorisation for Object required** – when the option is enabled then only users with proper Authorisation can use the key. The Authorisation must include Object type Positive rule for the object of the function.

Option **Authorisation for Function Parameter required** – when the option is enabled then users with proper Authorisation can use the key. The Authorisation must include Parameter type Positive rule for the parameter of the function.

Function Key functions

Function Key functions are available within selected objects. For example, key can be used for arming/disarming and then it should be configured on the level of Alarm Zone. Function Key functions are the same as Input functions (table 6) except for Power Supply object functions and toggle (status) type functions.

Local Commands

Local Command represents virtual object which can be triggered on the level of Access Point based on settings in Authentication Options tab (e.g. by card reading) or can be triggered by Global Command. The same as Inputs objects, Local Commands are used to start action in the system and type of action depends on the function assigned to particular command (e.g. door blocking). One or more functions can be assigned to single command. When multifunction command is applied then its triggering may start multiple actions in the system. In practical applications, Local Commands are mainly used to trigger input functions as a result of user identification (card or PIN) at Access Point (reader) instead of Input line triggering or Function Key pressing.

Area General

Text box **Name** – enables to name the command.

Text box **Description** – enables to enter custom description for the command.

Area Additional Options

Parameter **Activity Schedule** – enables assignment of schedule to specify when command can be used. It requires earlier defining of General Purpose Maintained type Schedule.

Option **Multifunction** – when the option is enabled then it is possible to specify the maximal number functions for assignment to the command.

Parameter **Function Limit** – specifies the maximal number of functions for assignment to the command.

Area Events

Option **Register event when command is used** – when the option is enabled then key pressing will generate an event in the system.

Parameter **Local Command Event** – enables to indicate what event is generated in the system when the key is used. It could be default event *[659]* or any other administrator defined event.

Local Command object can be further configured, mainly in regard of its function on the level of other objects e.g. Automation Point. Other parameters for such configuration are given below, while parameters specific for particular function are explained in the description of such function in the table 6.

Local Command when created is further assigned within Authentication Options on the level of Access Point. This assignment specifies the method to trigger Local Command (e.g. double card reading). Local Command can also be triggered on the level of Global Command which in turn can be triggered automatically be event(s) generated in the system.

roger

Area General

Parameter *Local Command* – enables to select Local Command object.

Parameter *Function* – enables to select function for the command. The list of all available functions is given in the table 6 below.

Parameter *Parameter* – specifies parameter of selected function. It is available for some functions only.

Option *Register Action Event* – when the option is enabled then command triggering generates event related to command function.

Parameter *Logic Function* – not used for Local Command.

Area Authorisation Options

Option *User authentication required* – when the option is enabled then users can use the command without Authorisation(s) assigned. It is enough that such users are equipped with Authentication Factors which are enrolled in the system.

Option *Authorisation for Access Point required* – when the option is enabled then only users with proper Authorisation can use the command. The Authorisation must include Access Point type Positive rule for the Access Point where the command is started.

Option *Authorisation for Object required* – when the option is enabled then only users with proper Authorisation can use the command. The Authorisation must include Object type Positive rule for the object where command is configured (e.g. Access Door).

Option *Authorisation for Function Parameter required* – when the option is enabled then users with proper Authorisation can use the key. The Authorisation must include Parameter type Positive rule for the parameter of the function triggered by command.

Local Commands functions

Local Command functions are available within selected objects. For example, command can be used for arming/disarming and then it should be configured on the level of Alarm Zone. Function Key functions are the same as Input functions (table 6) except for Power Supply object functions and toggle (status) type functions.

Outputs

Output represents object dedicated to control external electric device. Output function specifies situation (event) when output is triggered (e.g. door lock release as a result of access granting). The function can trigger output with various modulations. One or more functions can be assigned to single output. When multifunction output is applied then its triggering may be started by multiple actions in the system according to their priorities.

Area General

Text box *Name* – enables to name the output.

Text box *Description* – enables to enter custom description for the output.

Area Object

Parameter *Name* – enables selection of physical output.

Info box *Device* – specifies device with selected output.

Info box *Label* – specifies type of object.

Info box *Comment* – displays comment which was assigned to the output during low level configuration.

Info box *Type* – specifies type of output.

Info box *IP Address* – specifies IP address of host device (controller).

Info box *RS Address* – specifies RS485 address of device with the output.

Area Additional Options

Parameter *Activity Schedule* – enables assignment of schedule to specify when output can be triggered. It requires earlier defining of General Purpose Maintained type Schedule.

Parameter *Reset Schedule* – enables assignment of schedule to specify when output will be released (if triggered). It requires earlier defining of General Purpose Momentary type Schedule.

Option *Multifunction* – when the option is enabled then it is possible to specify the maximal number functions for assignment to the output.

Parameter *Function Limit* – specifies the maximal number of functions for assignment to the output.

Output object can be further configured, mainly in regard of its function on the level of other objects e.g. Access Door. Other parameters for such configuration are given below, while parameters specific for particular function are explained in the description of such function in the table 7.

Area General

Parameter *Output* – enables to select Output object.

Parameter *Function* – enables to select function for the Output. The list of all available functions is given in the table 7 below.

Area Triggering Options

Parameter *Priority* – specifies priority of function for multifunction output. The function with higher priority controls the output and overrides current signalling at the output.
Parameter *Triggering Method* – specifies method of output triggering. Available values:

- *Set output ON for period of time* – output is triggered for time specified by the parameter *Pulse Time*.
- *Set output ON for unlimited time* – output is triggered indefinitely.
- *Set output OFF* – output is released indefinitely.

Parameter *Pulse Time* – specifies total triggering time for *Set output ON for period of time* triggering method.
Parameter *Unit* – specifies time unit for *Pulse Time* parameter.

Area Modulation Options

Parameter *Type* – specifies output modulation e.g. one short pulse repeated every 1s.
Parameter *Frequency* – specifies frequency of modulation when *Custom* type is selected.
Parameter *Pattern* – specifies pattern of modulation when *Custom* type is selected.
Parameter *Number of Cycles* – specifies number of pattern repetitions when *Custom* type is selected.

Area Function Parameter

Enables selection of parameter for some of output functions e.g. Schedule for function *[017]*, intensity for function *[089]*, etc.

Output functions

Output functions are available within selected objects. For example, output line can be used to control door lock and then it should be configured on the level of Access Door.

Output functions are divided into event type which are triggered by state/event and status type which reflect particular state from trigger moment to release moment.

	Table 7 Output functions			
No.	Name	Type	Object	Description
1	Low Battery Status	Status	Power Supply	Triggered as long as low battery is detected.
2	Low Battery ON	Event	Power Supply	Triggered when low battery is detected.
3	Low Battery OFF	Event	Power Supply	Triggered when low battery is no longer detected.
4	Battery Failure Status	Status	Power Supply	Triggered as long as battery failure is detected.
5	Battery Failure ON	Event	Power Supply	Triggered when battery failure is detected.
6	Battery Failure OFF	Event	Power Supply	Triggered when battery failure is no longer detected.
7	AC Lost Status	Status	Power Supply	Triggered as long as 18VAC power supply is lost.
8	AC Lost ON	Event	Power Supply	Triggered when AC power supply lost is detected.
9	AC Lost OFF	Event	Power Supply	Triggered when AC power supply lost is no longer detected.
10	Delayed AC Lost Status	Status	Power Supply	Triggered as long as delayed AC power supply is lost.
11	Delayed AC Lost ON	Event	Power Supply	Triggered when delayed AC power supply lost is detected.
12	Delayed AC Lost OFF	Event	Power Supply	Triggered when delayed AC power supply lost is no longer detected.
13	Power Supply Overload Status	Status	Power Supply	Triggered as long as power supply unit overload is detected.
14	Power Supply Overload ON	Event	Power Supply	Triggered when power supply unit overload is detected.
15	Power Supply Overload OFF	Event	Power Supply	Triggered when power supply unit overload is no longer detected.
16	Calendar Status	Status	Main Board	Triggered on days specified by assigned Calendar. It requires earlier defining of Calendar.
17	Schedule Status	Status	Main Board	Triggered for time periods specified by assigned Schedule. It requires earlier defining of General Purpose Maintained type Schedule. Predefine Always and Never schedules cannot be applied.
18	Schedule ON	Event	Main Board	Triggered when schedule period/moment starts. It requires earlier defining of General Purpose Maintained type Schedule or General Purpose Momentary type Schedule. Predefine Always and Never schedules cannot be applied.
19	Schedule OFF	Event	Main Board	Triggered when schedule period ends. It requires earlier defining of General Purpose Maintained type Schedule. Predefine Always and Never schedules cannot be applied.
20	Controller Start	Event	Main Board	Triggered when MC16 controller is started.

21	Node Status	Status	Automation Node	Triggered as long as Automation Node is switched on.
22	Node ON	Event	Automation Node	Triggered when Automation Node is switched on.
23	Node OFF	Event	Automation Node	Triggered when Automation Node is switched off.
24	Node ON/OFF	Event	Automation Node	Triggered when Automation Node is switched on or switched off.
26	Door Status	Status	Access Door	Triggered as long as door is opened. It replicates input with the function *[130]* within the same Access Door.
27	Door Opened	Event	Access Door	Triggered when door is opened. It reports activation of input with the function *[130]* within the same Access Door.
28	Door Closed	Event	Access Door	Triggered when door is closed. It reports deactivation of input with the function *[130]* within the same Access Door.
29	Door Opened/Closed	Event	Access Door	Triggered when door is opened and closed. It reports activation and deactivation of input with the function *[130]* within the same Access Door.
30	Door Open Too Long Prealarm	Event	Access Door	Triggered as warning before actual Door Open Too Long Alarm. Activation moment depends on Access Door parameter *Door Open Too Long Prealarm Time*.
31	Door Lock	Status	Access Door	Triggered when access is granted at Access Door. The function is used to control door lock (door strike, maglock, etc.)
32	Door Open Too Long Alarm	Event	Access Door	Triggered when Door Open Too Long Alarm is raised. It depends on input with the function *[130]* and Access Door parameter *Door Open Too Long Time*.
33	Door Forced Alarm	Event	Access Door	Triggered when Door Forced Alarm is raised. The alarm is detected when access is not granted by controller but input with the function *[130]* is triggered.
34	Access Door Bell	Event	Access Door	Triggered when door bell is activated at Access Door i.e. input with the function *[131]* is triggered.
35	Read-in Door Lock Status	Status	Access Door	Triggered when access is granted by user identification at Access Point with the parameter *Read-in* or *Read-in/out*. The function is mainly used to control read-in/out portal such as turnstile, gate, etc. Contrary to function *[37]* it is used to control by means of status.

36	Read-out Door Lock Status	Status	Access Door	Triggered when access is granted by user identification at Access Point with the parameter *Read-out* or *Read-in/out*. The function is mainly used to control read-in/out portal such as turnstile, gate, etc. Contrary to function *[38]* it is used to control by means of status.
37	Read-in Door Lock	Event	Access Door	Triggered when access is granted by user identification at Access Point with the parameter *Read-in* or *Read-in/out*. The function is mainly used to control read-in/out portal such as turnstile, gate, etc. Contrary to function *[35]* it is used to control by means of pulse.
38	Read-out Door Lock	Event	Access Door	Triggered when access is granted by user identification at Access Point with the parameter *Read-out* or *Read-in/out*. The function is mainly used to control read-in/out portal such as turnstile, gate, etc. Contrary to function *[36]* it is used to control by means of pulse.
39	Wireless Door Lock	Event	Access Door	Triggered when access is granted. The function is dedicated to wireless locks of such systems as Aperio (ASSA ABLOY) or Clex Public (Uhlmann&Zacher).
41	Armed ON Mode Status	Status	Alarm Zone	Triggered as long as Alarm Zone is armed. The function operates inversely to function *[48]*.
42	Armed ON Mode	Event	Alarm Zone	Triggered when Alarm Zone is armed.
43	Armed OFF Mode	Event	Alarm Zone	Triggered when Alarm Zone is disarmed.
44	Armed ON/Armed OFF Mode	Event	Alarm Zone	Triggered when Alarm Zone is armed or disarmed.
45	Armed ON Mode Request	Event	Alarm Zone	Triggered when request to arm is started by means of input function *[107]* or *[109]*.
46	Armed OFF Mode Request	Event	Alarm Zone	Triggered when request to disarm is started by means of input function *[108]* or *[109]*.
47	Armed ON/Armed OFF Mode Request	Event	Alarm Zone	Triggered when request to arm or disarm is started by means of input function *[107]*, *[108]* or *[109]*.
48	Armed OFF Mode Status	Status	Alarm Zone	Triggered as long as Alarm Zone is disarmed. The function operates inversely to function *[41]*.
49	Intruder Alarm Status	Status	Alarm Zone	Triggered as long as Intruder Alarm is signalled. The alarm is started by input function *[220]* or *[221]* for the time specified by Alarm Zone parameter *Alarm Time [s]*.
50	Intruder Alarm ON	Event	Alarm Zone	Triggered when Intruder Alarm is raised by input function *[220]* or *[221]*.
51	Anti-passback Violation	Event	Access Zone	Triggered when Anti-passback rules are violated by a user at Access Point.

52	Occupancy Upper Limit ON	Event	Access Zone	Triggered when the number of users in Access Zones reaches value specified by the parameter *Upper Limit*.
53	Occupancy Lower Limit ON	Event	Access Zone	Triggered when the number of users in Access Zones reaches value specified by the parameter *Lower Limit*.
54	No Users in Access Zone ON	Event	Access Zone	Triggered when the last user leaves Access Zone.
55	No Users in Access Zone Status	Status	Access Zone	Triggered as long as there are no users in Access Zone.
56	Occupancy Upper Limit Status	Status	Access Zone	Triggered as long as the number of users in Access Zone reaches the value specified by the parameter *Upper Limit*.
57	Occupancy Lower Limit Status	Status	Access Zone	Triggered as long as the number of users in Access Zone reaches the value specified by the parameter *Lower Limit*.
58	Tamper Status	Status	Main Board	Triggered as long as Tamper Alarm is raised by input function *[133]*.
59	Tamper ON	Event	Main Board	Triggered when Tamper Alarm is raised by input function *[133]*.
61	T&A Event Registered	Event	Access Point	Triggered when Time&Attendance event is registered at Access Point.
62	Elevator Problem Status	Status	Access Point	Triggered as long as problem with elevator control is detected. The function is available only for MC16-EVK controllers and it is removed in RACS 5 v2 system.
63	Elevator Called	Event	Access Point	Triggered when elevator is called. The function is available only for MC16-EVK controllers and it is removed in RACS 5 v2 system.
64	Access Point Bell	Event	Access Point	Triggered when door bell is activated at Access Point i.e. input with the function *[159]* is triggered.
65	LED SYSTEM Status	Status	Access Point	Triggered as long as LED SYSTEM ⚡ (orange) indicator on one of terminals belonging to the Access Point is switched on. By default the indicator is used to signal various system functions including reader error.
66	LED OPEN Status	Status	Access Point	Triggered as long as LED OPEN 🔓 (green) indicator on one of terminals belonging to the Access Point is switched on. By default the indicator is used to signal access granting at Access Point.
67	LED ARMED Status	Status	Access Point	Triggered as long as LED ARMED ⚡ (red) indicator on one of terminals belonging to the Access Point is switched on. By default the indicator is used to signal that Access Point belongs to armed Alarm Zone.
68	LED DISARMED Status	Status	Access Point	Triggered as long as LED DISARMED ⚡ (green) indicator on one of terminals belonging to the Access Point is switched on. By default the indicator is used to signal that Access Point belongs to disarmed Alarm Zone.

69	BUZZER Status	Status	Access Point	Triggered as long as buzzer on one of terminals belonging to the Access Point is switched on. By default the buzzer is used to signal access granting, access denying, etc. at Access Point.
70	Access Granted at Access Point	Event	Access Point	Triggered when access granting results from use of input function *[151]*, *[152]*, *[175]* or *[176]*.
71	LED CARD PRESENT Status	Status	Access Point	Triggered as long as LED CARD PRESENT (green light line) indicator on terminal with card holder (e.g. MCT82M-IO-CH) is switched on. By default the green light line is used to signal authorised card in the holder.
72	LED CARD ABSENT Status	Status	Access Point	Triggered as long as LED CARD PRESENT (red light line) indicator on terminal with card holder (e.g. MCT82M-IO-CH) is switched on. By default the red light line is used to signal no authorised card in the holder.
73	Card in Holder Status	Status	Access Point	Triggered as long as authorised card is present in card holder of the terminal (e.g. MCT82M-IO-CH) belonging to Access Point.
74	Card in Holder ON	Event	Access Point	Triggered when authorised card is inserted into card holder of the terminal (e.g. MCT82M-IO-CH) belonging to Access Point.
75	Card in Holder OFF	Event	Access Point	Triggered when authorised card is removed from card holder of the terminal (e.g. MCT82M-IO-CH) belonging to Access Point.
76	Guard Tour Event Registered	Event	Access Point	Triggered when Guard Tour event is registered as a result of input function *[171]* activation.
77	Trace Event Registered	Event	Access Point	Triggered when Trace event is registered as a result of input function *[172]* activation.
78	Muster Event Registered	Event	Access Point	Triggered when Muster event is registered as a result of input function *[173]* activation.
79	Duress Event Registered	Event	Access Point	Triggered when Duress event is registered as a result of input function *[174]* activation.
80	Negative Access Mode	Event	Access Point	Triggered when Negative Access Mode is set at Access Point.
81	Positive Access Mode	Event	Access Point	Triggered when Positive Access Mode is set at Access Point.
82	Normal Access Mode	Event	Access Point	Triggered when Normal Access Mode is set at Access Point.
83	External Access Mode	Event	Access Point	Triggered when External Access Mode set at Access Point.
84	Delayed Access Mode	Event	Access Point	Triggered when Delayed Access Mode is set at Access Point.
85	Disabled Access Mode	Event	Access Point	Triggered when Disabled Access Mode is set at Access Point.

86	Access Request Pending Status	Status	Access Point	Triggered from the moment of user identification till access granting or denying for External Access Mode or Delayed Access Mode at Access Point.
87	Incoming Auto-arming Status	Status	Alarm Zone	Triggered as long as warning before Alarm Zone auto-arming is signaled. *Incoming Auto-arming Signaling Time* and other auto-arming parameters are configured within Alarm Zone.
88	Access Denied at Access Point	Event	Access Point	Triggered when access denying results from use of input function *[151]*, *[152]*, *[175]* or *[176]*.
89	Random Personal Check	Event	Access Point	Triggered when user is randomly selected for personal check after identification at Access Point. The probability is specified by function parameter *Intensity [%]*. Additionally the user can be denied access if Access Point option *Deny access on random personal check* is enabled.
90	Intruder Alarm OFF	Event	Alarm Zone	Triggered when Intruder Alarm is finished.
91	Intruder Alarm ON/OFF	Event	Alarm Zone	Triggered when Intruder Alarm is raised or finished.
92	Entry Delay Status	Status	Alarm Zone	Triggered as long as entry delay is signaled within Alarm Zone.
93	Entry Delay ON	Event	Alarm Zone	Triggered when entry delay is started within Alarm Zone.
94	Entry Delay OFF	Event	Alarm Zone	Triggered when entry delay is finished within Alarm Zone.
95	Entry Delay ON/OFF	Event	Alarm Zone	Triggered when entry delay is started or finished within Alarm Zone.
96	Ready to Arm Flag Status	Status	Alarm Zone	Triggered as long as Alarm Zone is ready to arm.
97	Ready to Arm Flag ON	Event	Alarm Zone	Triggered when Alarm Zone is ready to arm.
98	Ready to Arm Flag OFF	Event	Alarm Zone	Triggered when Alarm Zone is no longer ready to arm.
99	Ready to Arm Flag ON/OFF	Event	Alarm Zone	Triggered when Alarm Zone is ready to arm or is no longer ready to arm.
100	Incoming Auto-arming ON	Event	Alarm Zone	Triggered when warning before Alarm Zone auto-arming is started. *Incoming Auto-arming Signaling Time* and other auto-arming parameters are configured within Alarm Zone.
139	VDR Power Output Overload Status	Status	Power Supply	Triggered as long as VDR power output is overloaded.
140	VDR Power Output Overload ON	Event	Power Supply	Triggered when VDR power output is overloaded.
141	VDR Power Output Overload OFF	Event	Power Supply	Triggered when VDR power output is no longer overloaded.
142	TML Power Output Overload Status	Status	Power Supply	Triggered as long as TML power output is overloaded.

143	TML Power Output Overload ON	Event	Power Supply	Triggered when TML power output is overloaded.
144	TML Power Output Overload OFF	Event	Power Supply	Triggered when TML power output is no longer overloaded.
160	Connection with Peripheral Device Lost	Event	Main Board	Triggered when connection of controller with any device on RS485 bus is lost. Additionally delay can be defined to specify how long the connection must be lost to activate the output function. Similar function *[160]* is available.
212	Cafeteria Flag ON	Event	Access Point	Triggered when Cafeteria flag is switched on. The function is available only for MC16-HRC controllers.
213	Cafeteria Flag OFF	Event	Access Point	Triggered when Cafeteria flag is switched off. The function is available only for MC16-HRC controllers.
214	Cafeteria Flag ON/OFF	Event	Access Point	Triggered when Cafeteria flag is switched on or off. The function is available only for MC16-HRC controllers.
215	Cafeteria Flag Status	Status	Access Point	Triggered as long as Cafeteria flag is switched on. The function is available only for MC16-HRC controllers.
216	Luggage Service Flag ON	Event	Access Point	Triggered when Luggage Service flag is switched on. The function is available only for MC16-HRC controllers.
217	Luggage Service Flag OFF	Event	Access Point	Triggered when Luggage Service flag is switched off. The function is available only for MC16-HRC controllers.
218	Luggage Service Flag ON/OFF	Event	Access Point	Triggered when Luggage Service flag is switched on or off. The function is available only for MC16-HRC controllers.
219	Luggage Service Flag Status	Status	Access Point	Triggered as long as Luggage Service flag is switched on. The function is available only for MC16-HRC controllers.
224	Do Not Disturb Flag ON	Event	Access Point	Triggered when Do Not Disturb flag is switched on. The function is available only for MC16-HRC controllers.
225	Do Not Disturb Flag OFF	Event	Access Point	Triggered when Do Not Disturb flag is switched off. The function is available only for MC16-HRC controllers.
226	Do Not Disturb Flag ON/OFF	Event	Access Point	Triggered when Do Not Disturb flag is switched on or off. The function is available only for MC16-HRC controllers.
227	Do Not Disturb Flag Status	Status	Access Point	Triggered as long as Do Not Disturb flag is switched on. The function is available only for MC16-HRC controllers.
228	Assistance Flag ON	Event	Access Point	Triggered when Assistance flag is switched on. The function is available only for MC16-HRC controllers.
229	Assistance Flag OFF	Event	Access Point	Triggered when Assistance flag is switched off. The function is available only

				for MC16-HRC controllers.
230	Assistance Flag ON/OFF	Event	Access Point	Triggered when Assistance flag is switched on or off. The function is available only for MC16-HRC controllers.
231	Assistance Flag Status	Status	Access Point	Triggered as long as Assistance flag is switched on. The function is available only for MC16-HRC controllers.
232	Make Up Room Flag ON	Event	Access Point	Triggered when Make Up Room flag is switched on. The function is available only for MC16-HRC controllers.
233	Make Up Room Flag OFF	Event	Access Point	Triggered when Make Up Room flag is switched off. The function is available only for MC16-HRC controllers.
234	Make Up Room Flag ON/OFF	Event	Access Point	Triggered when Make Up Room flag is switched on or off. The function is available only for MC16-HRC controllers.
235	Make Up Room Flag Status	Status	Access Point	Triggered as long as Make Up Room flag is switched on. The function is available only for MC16-HRC controllers.
236	Service Flag ON	Event	Access Point	Triggered when Service flag is switched on. The function is available only for MC16-HRC controllers.
237	Service Flag OFF	Event	Access Point	Triggered when Service flag is switched off. The function is available only for MC16-HRC controllers.
238	Service Flag ON/OFF	Event	Access Point	Triggered when Service flag is switched on or off. The function is available only for MC16-HRC controllers.
239	Service Flag Status	Status	Access Point	Triggered as long as Service flag is switched on. The function is available only for MC16-HRC controllers.
240	Check-in Flag ON	Event	Access Point	Triggered when Check-in flag is switched on. The function is available only for MC16-HRC controllers.
241	Check-in Flag OFF	Event	Access Point	Triggered when Check-in flag is switched off. The function is available only for MC16-HRC controllers.
242	Check-in Flag ON/OFF	Event	Access Point	Triggered when Check-in flag is switched on or off. The function is available only for MC16-HRC controllers.
243	Check-in Flag Status	Status	Access Point	Triggered as long as Check-in flag is switched on. The function is available only for MC16-HRC controllers.
244	Connection with Communication Service Status	Status	Main Board	Triggered as long as the connection with communication service (RogerSVC) is correct.
245	Connection with Communication	Event	Main Board	Triggered when connection with communication service (RogerSVC) is lost.

	Service Lost			
246	Connection with Communication Service Restored	Event	Main Board	Triggered when connection with communication service (RogerSVC) is restored.
247	Occupancy Upper Limit (Prealarm) ON	Event	Access Zone	Triggered when the number of users in Access Zones reaches value specified by the parameter *Upper Limit (Prealarm)*.
248	Occupancy Lower Limit (Prealarm) ON	Event	Access Zone	Triggered when the number of users in Access Zones reaches value specified by the parameter *Lower Limit (Prealarm)*.
249	Occupancy Upper Limit (Prealarm) Status	Status	Access Zone	Triggered as long as the number of users in Access Zone reaches or exceeds value specified by the parameter *Upper Limit (Prealarm)*.
250	Occupancy Lower Limit (Prealarm) Status	Status	Access Zone	Triggered as long as the number of users in Access Zone reaches or falls below value specified by the parameter *Lower Limit (Prealarm)*.
251	Delayed Occupancy Lower Limit ON	Event	Access Zone	Triggered with a delay when the number of users in Access Zones is lower by one than the parameter *Lower Limit* and higher than zero. The function is not triggered when zone is empty. Delay in range of 0-254s (by default 30s) is specified with the parameter OLD= in OPTIONS.CFG text file on controller memory card.
252	Delayed Occupancy Lower Limit Status	Status	Access Zone	Triggered with a delay as long as the number of users in Access Zones is lower by one than the parameter *Lower Limit* and higher than zero. The function is not triggered when zone is empty. Delay in range of 0-254s (by default 30s) is specified with the parameter OLD= in OPTIONS.CFG text file on controller memory card.
253	Failed Attempts Limit	Event	Access Point	Triggered when failed attempt limit for user identification is reached. The limit is configured within Access Point configuration.
254	Access Point Disabled	Event	Access Point	Triggered when Access Point is disabled by input functions *[257], [259]* or as result of reaching failed attempt limit for user identification.
255	Access Point Enabled	Event	Access Point	Triggered when Access Point is enabled by input functions *[258], [259]* or when *Failed Attempts Blocking Time* elapses.
256	Access Point Disabled Status	Status	Access Point	Triggered as long as Access Point is disabled by input functions *[257], [259]* or as result of reaching failed attempt limit for user identification.
265	Occupancy Counter Value Manual Corrections Cleared	Event	Access Zone	Triggered when all modifications of Occupancy Upper Limit are cleared with input function *[262]*. The function is available only for MC16-AZC controllers.
266	Occupancy Counter Value without Manual Corrections Status	Status	Access Zone	Triggered as long as Occupancy Upper Limit in Access Zone is not modified with functions *[260], [261], [263]* and *[264]*. The function is available only for

				MC16-AZC controllers.
267	Occupancy Counter Value with Manual Corrections Status	Status	Access Zone	Triggered as long as Occupancy Upper Limit in Access Zone is modified with functions *[260]*, *[261]*, *[263]* and *[264]*. The function is available only for MC16-AZC controllers.
268	Connection with Indicated Peripheral Device Lost	Event	Main Board	Triggered when connection of controller with selected device on RS485 bus is lost. Additionally device RS485 address can be indicated and delay can be defined to specify how long the connection must be lost to activate the output function. Similar function *[160]* is available.

Automation Nodes

Automation Node represents virtual object which can be used for advanced control of Outputs which can be used to control external devices/systems. The node can be activated by Input, Function Key or Local Command.

Area General

Text box *Name* – enables to name the point.

Parameter *Group* – enables to assign node to previously created Automation Node Group.

Text box *LCD Message* – enables to specify node's name which will be used on display.

Parameter *Keypad Shortcut* – enables to select key which will correspond to the node when interactive options are applied.

Text box *Description* – enables to enter custom description for the node.

Area Triggering Options

Parameter *Default Time* – specifies default activation time of the node.

Parameter *Default Delay* – specifies default delay for node activation.

Option *Activation Extending* – when the option is enabled then input functions *[162]* and *[167]* can be used to extend activation of node by the time specified respectively with parameters *Default Time* and *Parametric Time* if the remaining time for node deactivation is lower than mentioned parameters. When node activation is extended then *Default Time* and *Parametric Time* parameters are not applied.

Area Additional Options

Parameter *Default State* – specifies default state of the node when it is not activated by function. Available values:

- *ON* – by default node is switched on.
- *OFF* – by default node is switched off.

Parameter *Activity Schedule* – enables assignment of schedule to specify when node can be triggered. It requires earlier defining of General Purpose Maintained type Schedule.

Area Events

Option *Register event when node is switched ON* – when the option is enabled then node switching on will generate an event in the system.

Parameter *Node ON Event* – enables to indicate what event is generated in the system when the node is switched on. It could be default event *[657]* or any other administrator defined event.

Option *Register event when node is switched OFF* – when the option is enabled then node switching off will generate an event in the system.

Parameter *Node OFF Event* – enables to indicate what event is generated in the system when the node is switched off. It could be default event *[658]* or any other administrator defined event.

Tab Inputs

The tab is available when an Automation Node is created and it enables to assign Input(s) to the node. Input parameters and functions are listed within the description of Input objects.

Tab Outputs

The tab is available when an Automation Node is created and it enables to assign Output(s) to the node. Output parameters and functions are listed within the description of Output objects.

Tab Function Keys

The tab is available when an Automation Node is created and it enables to assign Function Key(s) to the node. Function key parameters and functions are listed within the description of Function Key objects.

Tab Local Commands

The tab is available when an Automation Node is created and it enables to assign Local Commands to the node. Local Command parameters and functions are listed within the description of Local Command objects.

Access Zones

Access Zone represents an area with Access Points which are designated as Entry Points and Exit Points. Optionally the zone can also include Internal Points. When users identify at Entry Point then their presence in the zone is registered by the system and they can be granted access at Internal Points if they are assigned with proper Authorisations. When users identify at Exit Point then they are removed from zone register.

Access Zone can be used to enforce additional control of users movement including anti-passback, neighbouring zones, occupancy limits, group occupancy limits (only MC16-AZC) and usage limits (only MC16-AZC). More information on these functionalities is given in AN004 and AN031 application notes.

Note: Functionalities on the level of Access Zone concern identification and counting of Access Credentials. If each user has not more than single Access Credential assigned then the functionalities in fact concern users.

Area General

Text box *Name* – enables to name the zone.

Option *Group Occupancy Limits* – when enabled then group occupancy limits can be defined. The option is available only for MC16-AZC controllers.

Text box *LCD Message* – enables to specify zone's name which will be used on display.

Parameter *Keypad Shortcut* – enables to select key which will correspond to the zone when interactive options are applied.

Text box *Description* – enables to enter custom description for the zone.

Area Occupancy Count

Parameter *Upper Limit* – specifies maximal number of users inside Access Zone. When the limit is reached then users are denied access at Entry Point(s). The limit does not apply to Access Credentials with Master exemption and occupancy exemptions.

Parameter *Lower Limit* – specifies minimal number of users inside Access Zone. When the limit is reached then users are denied access at Exit Point(s). The limit does not apply to Access Credentials with Master exemption and occupancy exemptions.

Parameter *Upper Limit (Prealarm)* – specifies the number of users inside Access Zone which will trigger prealarm with output function *[247]* or *[249].*

Parameter *Lower Limit (Prealarm)* – specifies the number of users inside Access Zone which will trigger prealarm with output function *[248]* or *[250].*

Parameter *Occupancy Reset Schedule* – enables assignment of schedule to specify when occupancy register is cleared. It requires earlier defining of General Purpose Momentary type Schedule.

Area Anti-passback

Parameter *APB Mode* – specifies type of anti-passback for Access Zone. In general perspective Anti-passback (APB) prevents users from entering particular Access Zone again until they exit such zone thus preventing use of the same Access Credential by more than one user. Available values:

- *None* – APB is disabled.
- *Hard Anti-passback* – access is denied when APB rules are not followed and such violation is registered in the system.
- *Soft Anti-passback* – access is not denied when APB rules are not followed but such violation is registered in the system.

Parameter *APB Timeout [min]* – specifies expiry time for APB rule. When the time specified by the parameter elapses from the latest use of Authentication Factor then such factor can be used again without violating APB rules.

Parameter *APB Activity Schedule* – enables assignment of schedule to specify when APB rules are effective. It requires earlier defining of General Purpose Maintained type Schedule.

Parameter *APB Reset Schedule* – enables assignment of schedule to specify when APB register is cleared. It requires earlier defining of General Purpose Momentary type Schedule.

Area Neighboring Options

Option ***Do not allow to enter this zone from not neighboring zone*** – when the option is enabled then user is denied access at Entry Point(s) of Access Zone if user's current zone is not neighboring to the zone which user attempts to enter. Zones are configured as neighboring by configuration of Access Points. If particular Access Point is configured as Entry Point to zone A and at the same such Access Point is configured as Exit Point from zone B than both zones are neighboring. Neighboring options can be used to restrict and enforce user movement routes in premises.

Option ***Do not allow to exit this zone to not neighboring zone*** – when the option is enabled then user is denied access at Exit Point(s) of Access Zone if user's current zone is not neighboring to the zone which user attempts to enter. Zones are configured as neighboring by configuration of Access Points. If particular Access Point is configured as Entry Point to zone A and at the same such Access Point is configured as Exit Point from zone B than both zones are neighboring. Neighboring options can be used to restrict and enforce user movement routes in premises.

Area Credential Usage Reset Schedules

Parameter ***Usages Remaining Reset Schedule*** – enables assignment of schedule to specify when parameter *Usages Remaining* which is configured for particular Access Credentials by means of command *Set usage limits* will be reset. It requires earlier defining of General Purpose Momentary type Schedule. The parameter is available only for MC16-AZC controllers.

Parameter ***Days Remaining Reset Schedule*** – enables assignment of schedule to specify when parameter *Days Remaining* which is configured for particular Access Credentials by means of command *Set usage limits* will be reset. It requires earlier defining of General Purpose Momentary type Schedule. The parameter is available only for MC16-AZC controllers.

Parameter ***Absentee Time Reset Schedule*** – enables assignment of schedule to specify when parameter *Absentee Time* which is configured for particular Access Credentials by means of command *Set usage limits* will be reset. It requires earlier defining of General Purpose Momentary type Schedule. The parameter is available only for MC16-AZC controllers.

Tab Entry Points

The tab is available when an Access Zone is created and it enables to select which Access Points will function as Entry Points to the zone.

Tab Exit Points

The tab is available when an Access Zone is created and it enables to select which Access Points will function as Exit Points from the zone.

Tab Internal Points

The tab is available when an Access Zone is created and it enables to select which Access Points will function as Internal Points inside the zone. User can be granted access at Internal Point only if according to occupancy register such user is inside the zone i.e. user was granted access at Entry Point of the zone.

Tab Inputs

The tab is available when an Access Zone is created and it enables to assign Input(s) to the zone. Input parameters and functions are listed within the description of Input objects.

Tab Outputs

The tab is available when an Access Zone is created and it enables to assign Output(s) to the zone. Output parameters and functions are listed within the description of Output objects.

Tab Function Keys

The tab is available when an Access Zone is created and it enables to assign Function Key(s) to the zone. Function key parameters and functions are listed within the description of Function Key objects.

Tab Local Commands

The tab is available when an Access Zone is created and it enables to assign Local Commands to the zone. Local Command parameters and functions are listed within the description of Local Command objects.

Tab Group Occupancy Limits

The tab is available when an Access Zone is created and it enables to define Group Occupancy Limits. The tab is available only for MC16-AZC controllers.

Parameter ***User Group*** – enables to select User Group for further configuration of occupancy limits.

Parameter *Group Upper Limit* – specifies the maximal number of users from certain group inside Access Zone. When the limit is reached then users are denied access at Entry Point(s). The limit does not apply to Access Credentials with Master exemption and occupancy exemptions.

Parameter *Group Lower Limit* – specifies the minimal number of users from certain group inside Access Zone. When the limit is reached then users are denied access at Exit Point(s). The limit does not apply to Access Credentials with Master exemption and occupancy exemptions.

Alarm Zones

Alarm Zone represents area with Access Points which are designated as Arming Points. Access Points belonging to Alarm Zone are armed and disarmed concurrently and current arming mode is presented on LED indicators of MCT and PRT readers.

Alarm Zones can be applied in integration with intruder alarm systems, for alarm system functionalities of RACS 5 system and for additional access control. When adequate option is enabled then armed Access Point can deny access till their disarming while arming/disarming Authorisation can be condifured and assigned to users individually. More information on Alarm Zones is given in AN027 application note.

Area General

Text box *Name* – enables to name the zone.

Text box *LCD Message* – enables to specify zone's name which will be used on display.

Parameter *Keypad Shortcut* – enables to select key which will correspond to the zone when interactive options are applied.

Text box *Description* – enables to enter custom description for the zone.

Parameter *Parent* – enables to select Alarm Zone which will be used in hierarchy as superordinate zone.

Parameter *Auto-arming Schedule* – enables assignment of schedule to specify when Alarm Zone is automatically armed. It requires earlier defining of General Purpose Momentary type Schedule.

Parameter *Quick Disarming* – enables automatic disarming when access is granted.

Option *Disable physical access when zone armed* – when the option is enabled then Access Points of armed Alarm Zone deny access till zone disarming.

Area Auto-arming Options

Parameter *Incoming Auto-arming Signalling Time [min]* – specifies how many minutes before planned arming the warning is generated on Arming Points by means of LED STATUS (orange) indicators and by means of input function *[87]* or *[100]*.

Parameter *Auto-arming delay when zone not ready for arming [min]* – specifies how much the auto-arming is delayed when input function *[105]* is triggered in the moment of planned arming.

Parameter *Auto-arming delay on manual request [min]* – specifies how much the auto-arming is delayed when during auto-arming warning the input function *[106]* is used.

Option *Postpone auto-arming after physical access is granted* – when the option is enabled then auto-arming can be delayed not only by function *[106]* but also by access granting at Arming Point.

Area Alarm Functions

Parameters in this area are mainly dedicated to intruder alarm functionality in RACS 5 system with MC16-IAC controller(s).

Parameter *Alarm Time [s]* – specifies alarm signalling time triggered by input function *[220]* or *[221]*.

Parameter *Time Between Alarms [min]* – specifies minimal time between successive intruder alarms.

Parameter *Entry Delay [s]* – specifies delay in detection of alarm from input lines with functions *[221]*.

Parameter *Alarm Limit* – specifies maximal number of alarms for intruder detection.

Parameter *Intruder Detection Limit* – specifies maximal number of activations of input lines with functions *[220]* and *[221]*.

Tab Arming Points

The tab is available when an Alarm Zone is created and it enables to select which Access Points will function as Arming Points of the zone.

Tab Inputs

The tab is available when an Alarm Zone is created and it enables to assign Input(s) to the zone. Input parameters and functions are listed within the description of Input objects.

Tab Outputs

The tab is available when an Alarm Zone is created and it enables to assign Output(s) to the zone. Output parameters and functions are listed within the description of Output objects.

Tab Function Keys

The tab is available when an Alarm Zone is created and it enables to assign Function Key(s) to the zone. Function key parameters and functions are listed within the description of Function Key objects.

Tab Local Commands

The tab is available when an Alarm Zone is created and it enables to assign Local Commands to the zone. Local Command parameters and functions are listed within the description of Local Command objects.

Displays

Display is a logical object representing physical display of peripheral device (e.g. MCT88M-IO display) connected to MC16 controller. Such display can present not only its internal data but also messages from MC16 controller. More information on displays is given in AN011 application note.

Power Supplies

Power Supply is a logical object representing physical power supply unit of MC16 controller or other external device. Inputs and Outputs which are configured on the level of Power Supply are mainly used to monitor its status.

VISO software offers command for reading voltage of battery connected to power supply unit. It concerns batteries connected directly to MC16 controllers and batteries connected to such peripheral devices of the controller as MCX expanders and RWL locks.

Access Credentials and Access Users

In RACS 5 system an Access User can be assigned with multiple Access Credentials. Access Credential is a logical object which includes Authorisations (e.g. access rights at Access Door) which define user rights and it includes Authentication Factors (e.g. proximity cards) which are used to identify user in the system. Single MC16 v1.0 controller in RACS 5 v1 system supports up to 8000 Access Credentials (16 000 Authentication Factors) while in MC16 v1.1 controller in RACS 5 v2 system supports up to 12 000 Access Credentials (24 000 Authentication Factors). In case of MC16-AZC controllers it is possible to define credential usage limits on entry to Access Zone both in regard of their number and time. These usage limits are explained in AN031 application note.

Area General

Text box **Name** – enables to name the credential.

Parameter **Group** – enables to assign the credential to special group such as Visitor or Guest.

Parameter **Belongs to** – enables to assign the credential to Access User or Access User Group.

Parameter **Valid from** – specifies starting date and time for credential validity in the system.

Parameter **Valid to** – specifies ending date and time for credential validity in the system.

Area Additional Options

Parameter **Status** – specifies credential status. Available values:

- **Active** – Access Credential is valid in the system.
- **Inactive** – Access Credential is invalid in the system.

Parameter **Thread Level** – specifies credential access level. If credential's Thread Level is lower than Access Point's Thread Level then access is denied regardless of credential Authorisations.

Parameter **Elevator Call Type** – specifies type of elevator calling in case of integration with Kone Destination system elevators based on MC16-EVK controllers. The parameter was removed in RACS 5 v2 system.

Tab Exemptions

Option **Master Exemption** – when the option is enabled then the credential includes all possible Authorisations on the level of access controller.

Option **Anti-passback Exemption** – when the option is enabled then the credential is not affected by anti-passback rules on the level of Access Zones.

Option ***Occupancy Count Exemption*** – when the option is enabled then the credential is not recorded in occupancy register and consequently is not taken into account on the level of Access Zone registers and counters.

Option ***Occupancy Count Limit Exemption*** – when the option is enabled then the credential is not affected by occupancy limits on the level of Access Zones.

Option ***Perimeter Zone Exemption*** – when the option is enabled then the credential is not affected by limits on the level of Perimeter Zones.

Tab Description

Enables to enter custom description for the credential.

Tab OTIS Integration

The tab includes options related to OTIS elevator integration and it is available only if such integration is enabled according to AN039 application note.

Tab Authorisations

The tab is available when an Access Credential is created and it enables to select which Authorisations will be assigned to the credential. Such Authorisations can also be individually enabled and disabled.

Tab Authorisation Groups

The tab is available when an Access Credential is created and it enables to select which Authorisation Groups will be assigned to the credential. Such Authorisation Groups can also be individually enabled and disabled.

Tab Authentication Factors

The tab is available when an Access Credential is created and it enables to add Authentication Factors to the credential (max. 8)..

Authentication Factors

Authentication Factor is an element for user identification at Access Points. Typical factors are proximity cards, PINs, fingerprints, car license plates, mobile devices with RMK app and NFC or BLE technology. Authentication Factors are defined and assigned on the level of Access Credentials while cards can also be defined on the level of Card Box.

Authentication Policies

Authentication Policy includes Authentication Steps which define Authentication Factor Types for user identification at Access Point. Default Authentication Policy is Card or PIN. Other pre-programmed policies e.g. Card and PIN are available and it is possible to define own policy as well.

Area General

Text box ***Name*** – enables to name the policy.

Option ***Enabled*** – when the option is enabled then the policy is valid in the system.

Text box ***LCD Message*** – enables to specify policy's name which will be used on display.

Parameter ***Keypad Shortcut*** – enables to select key which will correspond to the policy when interactive options are applied.

Text box ***Description*** – enables to enter custom description for the policy.

Area Authentication Steps

Parameters ***Step 1*** - ***Step 4*** – enable to select Authentication Factor Type for particular step of the Authentication Policy. Up to four steps can be defined.

Area Advanced Options

Option ***Order Enforced*** – when the option is enabled then user must not only use all required Authentication Factor Types but they also must be exactly in the order specified for the policy.

Parameter ***Timeout [s]*** – specifies maximal total time for completion of user identification.

Parameter ***Alternative Authentication Policy*** – specifies alternative policy for the primary policy.

Authorisations

Authorisation defines User rights to start action by activation of input function(s). Authorisations can be assigned to Access User, Access Credential belonging to User and User Group. If Authorisation is assigned to User then it is inherited by all Access Credentials belonging to the user. The same Authorisation can be assigned to multiple Access Credentials, Access Users and Access User Groups. Authorisation may pertain to particular input function or group of such functions. Authorisation may include Positive Rules which define conditions to start action and Negative Rules which define when the action cannot be started. Negative Rules have higher priority than Positive Rules.

Authorisations are necessary to start an action both by user identification at Access Point and by Remote Command. Authorisation may also be necessary to use Inputs, Function Keys and Local Command if they require user authentication.

Authorisations are divided into Basic Authorisations which concern such function groups as among others physical access, arming control, automation, etc. and Advanced Authorisations which concern particular input functions (table 6) and enable to define rules on the level of Objects, Access Points and Function Parameters. More information on Authorisations is given in AN003 application note.

Basic Authorisations

Area General

Option **Enabled** – when the option is enabled then the Authorisation is valid in the system.

Text box **Name** – enables to name the Authorisation.

Parameter **Type** – enables to select function group for the Authorisation e.g. Physical Access. List of elements in the area *Allowed Object* depends on this parameter.

Parameter **Valid from** – specifies starting date and time for Authorisation validity in the system.

Parameter **Valid to** – specifies ending date and time for Authorisation validity in the system.

Text box **Description** – enables to enter custom description for the Authorisation.

Area Allowed Objects

This area contains list of objects which can be selected for the Authorisation. For example when *Physical Access Type* is selected then the area will contain list of Access Points which can be selected and assigned with General Purpose Maintained type Schedules to define rules of the Authorisation.

Advanced Authorisations

Area General

Option **Enabled** – when the option is enabled then the Authorisation is valid in the system.

Text box **Name** – enables to name the Authorisation.

Parameter **Type** – specifies type of Authorisation. Available values:

- **Main** – default value applied in most cases when Authorisation is defined.
- **Complementary** – value which is used in some scenarios concerning access control in elevators and lockers.

Parameter **Valid from** – specifies starting date and time for Authorisation validity in the system.

Parameter **Valid to** – specifies ending date and time for Authorisation validity in the system.

Text box **Description** – enables to enter custom description for the Authorisation.

Area Details

Parameter **Refers to** – specifies type of action for the Authorisation. Available values:

- **Function** – when selected then Authorisation will concern specific input function which can be selected in the next step
- **Function Group** – when selected then Authorisation will concern group of functions (e.g. Physical Access) which can be selected in the next step.

Parameter **Action** – specifies function or group of functions for the Authorisation.

Area Advanced Options

Option **Includes authorisation for all rules** – when the option is enabled then the Authorisation will include all Positive Rules defined in full range i.e. the Authorisation will allow to start action (function) without any limits in regard of Objects, Access Points and Function Parameters.

Option ***Includes authorisation for all Access Points*** – when the option is enabled then the Authorisation will include Positive Rule for all Access Point i.e. the action (function) can be started without any limits in regard of Access Points.

Option ***Includes authorisation for all Function Parameters*** – when the option is enabled then the Authorisation will include Positive Rule for all Function Parameters i.e. the action (function) can be started without any limits in regard of Function Parameters.

Tab Negative Rules

The tab is available when an Advanced Authorisation is created and it enables to define Negative Rules in regard of Objects, Access Points and Function Parameters. Negative Rules have higher priority than Positive Rules.

Tab Positive Rules

The tab is available when an Advanced Authorisation is created and it enables to define Positive Rules in regard of Objects, Access Points and Function Parameters. Positive Rules have lower priority than Negative Rules.

Schedules

Schedule allows to make the system operation dependent on week day and day time. Schedules can be applied to multiple functions of the system including Authorisations. Schedule status can be presented on Output(s) and consequently used to control external devices and systems. Following Schedule types are available on the level of access controller.

- General Purpose Maintained
- Door Mode
- Time&Attendance Mode
- Authentication Policy
- General Purpose Momentary

Calendars

Calendar allows to alter system operation during holidays. They can be used to define exceptions to Schedules and consequently affect Authorisations which use such Schedules. Calendars can be defined for many years. Calendar status can be presented on Output(s) and consequently used to control external devices and systems.

5. SPECIFICATION

Table 8. Specification	
Supply voltage	17-22VAC, nominal 18VAC 11.5V-15VDC, nominal 12VDC, 22-26VDC, nominal 24VDC
Current consumption	50mA for 18VAC (no loads on AUX/TML outputs) 25mA for 24VDC (no loads on AUX/TML outputs)
Backup battery	Dry gel battery with a final charging voltage of 13.8V, charging current approx. 300mA
Inputs	Eight inputs (IN1-IN8) internally connected to the power supply plus through a 5.6kΩ resistor. Approx. 3.5V triggering level for NO and NC inputs.
Relay outputs	Two relay outputs (REL1, REL2) with single NO/NC contact 30V/1.5A rated
Transistor outputs	Eight open collector transistor outputs (OUT1-OUT6, CLK, DTA) 15VDC/150mA rated.
Power supply outputs	Two power outputs: 12VDC/0.2A (TML) and 12VDC/1A (AUX)
Distances	1200m for RS485 150m for and RACS CLK/DTA and Wiegand Power supply: according to AN022 application note

IP Code	IP00
Environmental class (acc. to EN 50131-1)	Class I, indoor general conditions, temperature: +5°C to +40°C, relative humidity: 10 to 95% (no condensation)
Dimensions H x W x D	72 x 175 x 30 mm
Weight	approx. 200g
Certificates	CE

6. ORDERING INFORMATION

All versions of MC16 controller are based on the same hardware and firmware while their functionalities are specified by license file on memory card with the exception of MC16-AZC controller in RACS 5 v2 system which requires dedicated firmware and additional entry in its license file. Each version includes various types of controllers. Following versions of MC16 controllers are available:

- MC16-PAC physical access controllers
- MC16-AZC parking access controllers
- MC16-LRC locker access controllers
- MC16-HRC hotel access and automation controllers
- MC16-EVC and MC16-EVK elevator access controllers
- MC16-BAC building automation controllers
- MC16-IAC alarm zone controllers
- MC16-SVC service controller

Additionally MC16-RAW modules are offered. They require firmware and license file upload for proper operation as one of available version of MC16 controller.

Parameters which are given in tables below represent maximal values and their actual application usually requires connection of peripheral devices (MCT, MCX). It is possible to upgrade from lower to higher type of controller e.g. MC16-PAC-4 -> MC16-PAC-8 and it requires ordering and then uploading of new license. When license file is ordered then it is necessary to submit MAC address of MC16 to Roger company.

MC16-PAC controllers

MC16-PAC controllers are most widely used controllers in RACS 5 system. They are mainly used to offer physical access control in premises. Various installation scenarios are presented in AN002 application note. Particular types of controllers differ by the number of controlled doors (max. 16).

Additionally in RACS 5 v2 system every MC16-PAC controller is offered in two versions i.e. ST and EX. MC16-PAC controllers in EX version can be used with ST (Standard) and EX (Enterprise) versions of VISO v2 management software while controllers in ST version can only be used with ST version of the software. More information on possibilities, limitations, licensing and migration of RACS 5 system is given in AN015 application note.

Table 9. MC16-PAC types				
Type	MC16-PAC-1	MC16-PAC-2	MC16-PAC-4	MC16-PAC-N
Access Doors	1	2	4	N (≤16)
Access Points	2	4	8	2 x N
Inputs	8	12	24	6 x N
Outputs	8	8	16	4 x N
Function Keys	8	16	32	8 x N
Local Commands	2	4	8	2 x N
Access Zones	2	4	8	2 x N
Alarm Zones	2	4	8	2 x N

Automation Nodes	2	4	8	2 x N
Power Supplies	2	4	8	2 x N
Access Doors per Access Points	1	1	1	1

MC16-PAC-KIT installation sets

MC16-PAC controllers are offered individually and as elements of MC16-PAC-KITs which simplify RACS 5 system designing and installation. They can to be used to create dispersed system to ensure higher reliability than centralized system. They provide high resistance to tampering and offer simple and efficient power supplies. More information on MC16-PAC-KITs is given in their installation manuals.

MC16-AZC controllers

MC16-AZC controllers are mainly used at car parks. In RACS 5 v1 system they offer the same functionalities as MC16-PAC controllers and some additional ones in regard of advanced control of occupancy in Access Zone. In RACS 5 v2 system, MC16-AZC controllers require dedicated firmware and they do not support Automation Nodes. More information on the application of MC16-AZC controllers is given in AN031 application note. Particular types of controllers differ by the number of controlled doors (max. 16).

Table 10. MC16-AZC types				
Type	MC16-AZC-1	MC16-AZC-2	MC16-AZC-4	MC16-AZC-N
Access Doors	1	2	4	N (≤16)
Access Points	2	4	8	2 x N
Inputs	8	12	24	6 x N
Outputs	8	8	16	4 x N
Function Keys	4	8	16	4 x N
Local Commands	2	4	8	2 x N
Access Zones	2	4	8	2 x N
Alarm Zones	2	4	8	2 x N
Automation Nodes	2	4	8	2 x N
Power Supplies	2	4	8	2 x N
Access Doors per Access Points	1	1	1	1

MC16-LRC controllers

MC16-LRC controllers are dedicated to lockers. They offer wired access control based on MCT terminals. More information on MC16-LRC controllers is given in AN029 application note. Particular types of controllers differ by the number of controlled lockers (max. 64).

Table 11. MC16-LRC types				
Type	MC16-LRC-8	MC16-LRC-16	MC16-LRC-32	MC16-LRC-64
Access Doors	8	16	32	64
Access Points	2	4	8	16
Inputs	16	32	64	128
Outputs	16	32	64	128

Function Keys	4	8	16	32
Local Commands	2	4	8	16
Access Zones	0	0	0	0
Alarm Zones	0	0	0	0
Automation Nodes	1	2	2	2
Power Supplies	2	4	8	16
Access Doors per Access Points	8	16	32	64

MC16-HRC controllers

MC16-HRC controllers and HR type terminals (e.g. MCT86M-IO-CH-HR) are dedicated to hotel applications. More information on MC16-HRC controllers is given in AN033 application note. Particular types of controllers differ by the number of controlled hotel rooms (max. 4).

Table 12. MC16-HRC types				
Type	MC16-HRC-1	MC16-HRC-2	MC16-HRC-3	MC16-HRC-4
Access Doors	1	2	3	4
Access Points	2	4	6	8
Inputs	8	12	18	24
Outputs	8	8	12	16
Function Keys	4	8	12	16
Local Commands	2	4	6	8
Access Zones	2	4	6	8
Alarm Zones	2	4	6	8
Automation Nodes	2	4	6	8
Power Supplies	2	4	6	8
Access Doors per Access Points	1	1	1	1

MC16-EVC and MC16EVK controllers

MC16-EVC controllers are dedicated to universal access control in elevators from various manufacturers. More information on MC16-EVC controllers is given in AN030 application note. Particular types of MC16-EVC controllers differ by the number of controlled floors (max. 64).

MC16-EVK controllers are dedicated for integration with Kone Destination elevator system from KONE company. There is one type of MC16-EVK controllers and it enables access control for up to 64 floors. These devices are not supported in RACS 5 v2 system.

Table 13. MC16-EVC types				
Type	MC16-EVC-8	MC16-EVC-16	MC16-EVC-32	MC16-EVC-64
Access Doors	8	16	32	64
Access Points	1	1	1	1
Inputs	8	8	8	8
Outputs	16	32	64	128

Function Keys	8	8	8	8
Local Commands	4	4	4	4
Access Zones	0	0	0	0
Alarm Zones	0	0	0	0
Automation Nodes	2	2	2	2
Power Supplies	2	4	8	16
Access Doors per Access Points	8	16	32	64

MC16-BAC controllers

MC16-BAC controller are dedicated to building automation control by means of Inputs and Outputs operated on the level of Automation Nodes. Particular types of controllers differ by the number of controlled Automation Nodes (max. 64).

Table 14. MC16-BAC types				
Type	MC16-BAC-8	MC16-BAC-16	MC16-BAC-32	MC16-BAC-64
Access Doors	0	0	0	0
Access Points	4	8	16	32
Inputs	16	32	64	128
Outputs	16	32	64	128
Function Keys	16	32	64	128
Local Commands	4	8	16	32
Access Zones	0	0	0	0
Alarm Zones	0	0	0	0
Automation Nodes	8	16	32	64
Power Supplies	4	8	16	32

MC16-IAC controllers

MC16-IAC controllers are dedicated to advanced control of Alarm Zones in RACS 5 system and they offer intruder alarm system functionalities. Particular types of controllers differ by the number of controlled Alarm Zones (max. 16).

Table 15. MC16-IAC types				
Type	MC16-IAC-2	MC16-IAC-4	MC16-IAC-8	MC16-IAC-16
Access Doors	0	0	0	0
Access Points	4	8	16	32
Inputs	16	32	64	128
Outputs	16	32	64	128
Function Keys	16	32	64	128
Local Commands	4	8	16	32
Access Zones	0	0	0	0

Alarm Zones	2	4	8	16
Automation Nodes	8	16	32	64
Power Supplies	4	8	16	32

MC16-SVC controllers

MC16-SVC controllers are dedicated to demo or service operation. The controller is delivered with a set of service licenses that enable its switching to an operating mode compatible with such controllers as MC16-PAC-16, MC16-LRC-64, MC16-EVC-64 or MC16-AZC-16. The operation of MC16-SVC controller is limited in time. More information on the controller is given in its installation manual.

7. PRODUCT HISTORY

Table 16. Product history		
Version	Date	Description
MC16 v1.0	06/2016	The first commercial version of product.
MC16 v1.1	02/2017	Extended RAM and FLASH memory onboard.

This symbol placed on a product or packaging indicates that the product should not be disposed of with other wastes as this may have a negative impact on the environment and health. The user is obliged to deliver equipment to the designated collection points of electric and electronic waste. For detailed information on recycling, contact your local authorities, waste disposal company or point of purchase. Separate collection and recycling of this type of waste contributes to the protection of the natural resources and is safe to health and the environment. Weight of the equipment is specified in the document.

Contact:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Fax: +48 55 272 0133
Tech. support: +48 55 267 0126
E-mail: support@roger.pl
Web: www.roger.pl