MREx 73

APS mini Plus reader modules

User's guide

(Date of release: 2019/06/03, valid for FW version 5.12)

1 Content

2 Product description

The *MREx 73* [1] reader modules (125 kHz readers with an embedded single door controller) are designed for connection to the RS 485 bus of the *APS mini Plus* access control system, or for standalone operation. It is possible to connect up to 32 reader modules to a single line of the APS mini Plus system. In effect the number of lines is not limited.

The reader module is available in various modifications differing in the way of use.

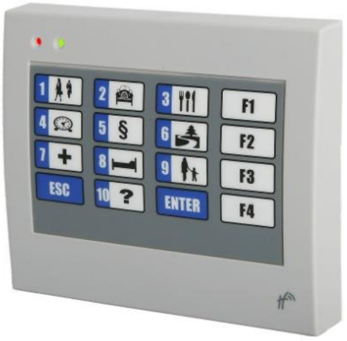
Pic. 1: MREM 73

2.1 MREM 73 reader module

Standard reader module for the APS mini Plus system; the user's identity is verified by reading an ID media (*Pic.1*).

2.2 MRED 73 reader module

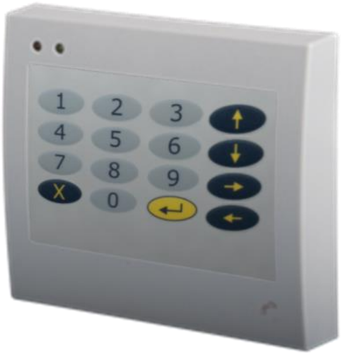
Reader module with a reason keypad (*Pic.2*); the user may enter an operation code by pressing a key, e.g. a reason to leave the building. The module is designed mainly for T&A applications.



Pic. 2: MRED 73

2.3 MREP 73 reader module

Reader module with a PIN keypad (*Pic.3*); uses the combination of ID media and a PIN code for user identification.



Pic. 3: MREP 73

[1] Commercial designation of available versions is described in *table 1*.

3 Technical parameters

3.1 Product version

Product version	Product designation	Keypad layout	Catalogue number	Module features [2]	
				TF	EM
	MREM 73 – TF	*N/A*	53473000	✓	✗
	MRED 73 – TF	*Reason keypad*	53473200	✓	✗
	MREP 73 – TF	*PIN keypad*	53473400	✓	✗
	MREM 73 – EM	*N/A*	53473001	✓	✓
	MRED 73 – EM	*Reason keypad*	53473201	✓	✓
	MREP 73 – EM	*PIN keypad*	53473401	✓	✓

Table 1: Product version

[2] *TF* – TECHFASS factory 125 kHz ID media reading; *EM* – 125 kHz ID media reading;

3.2 Technical features

Technical features	Supply voltage		8 ÷ 15 VDC
	Current demand	Typical	80 mA
		Maximal	120 mA
	Keypad layout	MREM 73	No keypad
		MRED 73	Reason keypad, 16 keys
		MREP 73	PIN keypad, 16 keys
	ID technology, typical reading range	EM Marin	8 cm (with ISO card)
	Real-time clock		Yes, with 24 hrs. back-up
	Memory	Cards	2,000 ID, 2 programming cards
		Events	3,400
		Time schedules	64
	Inputs	1st input	Logical potential-free contact
		2nd input	Logical potential-free contact
	Outputs	Door lock	Relay NC/NO, 2A/24V
		Alarm	Transistor output 5V/5mA
	I/O Port	External device	Ext. tamper / ext. reader buzzer control / module disable function / reading synchronization MASTER/SLAVE modes
	Indicators		3x LED 1x PIEZO
	Tamper protection		Reed contact
	Communication interface		RS 485
	Alternative data input / output		WIEGAND (configurable)

Table 2: Technical features

3.3 Special accessories

Accessories	MAG	51900200	Magnet for reed contact
	WIO 22	51901200	Remote control module, 2x relay

Table 3: Special accessories

3.4 Using WIO 22 module for remote output control

The *WIO 22* remote control *WIEGAND* relay module is designated for secure output control of APS system reader modules. The door open or other functions can be controlled from the module located inside the secure area, while the reader module can be located in the non-secure area.

The module is controlled by *WIEGAND* signal directly from the reader module working in standard operating mode. The module must be paired with appropriate reader module before use.

3.5 Mechanical design

Mechanical design	Weight		0.25 kg
	Operating temperature		-25 ÷ 60 °C
	Humidity		Max 95%, non-condensing
	Housing	MREM 73	IP 54, IK 07
		MRED 73, MREP 73	IP 52
	Pigtail		0.5 m
	Color		Light grey
	Dimensions		105x90x20 mm

Table 4: Mechanical design

4 Installation

4.1 Wiring description

Wiring description	Color	Function	Color	Function
	Red	Power sup. +8 ÷ +15 VDC	Green white	WIEGAND data 0
	Red blue	Power sup. +8 ÷ +15 VDC	Brown green	WIEGAND data 1
	Green	I/O Port 3	Yellow	Input 1 (IN1)
	Blue	GND (0 V)	Grey	Input 2 (IN2)
	Black	A wire - RS 485 line	Violet	NO relay contact
	White	B wire - RS 485 line	Brown	C relay contact
	Pink	Alarm output (AUX)	Grey pink	NC relay contact

Table 5: Wiring description

4.2 Standard connection

Connection	Input 1	Door contact, active when door closed; REX button
	Input 2	Request to exit button or handle contact; Tamper; Disabling function; active on 0 VDC
	Output 1 (relay)	Door lock control
	Alarm output	Low power transistor output (+5 V in any alarm state)
	I/O Port 3	External tamper (Standard operating mode) External reader buzzer control (op. mode with entry reader) Disabling function Reading synchronization: MASTER / SLAVE mode

Table 6: Standard connection

The door monitoring contact (IN1) is operational after its first change of status since switching on the module. Full door lock timing acc. to *tab. 8* is used when the door status contact is not installed and no Forced Door and Door Ajar alarms are triggered.

4.3 LED Indicators

LED indicators	Left LED	Red	Continuously lit	Online operating mode via RS 485
			Flashing with 4 s period	Offline operating mode
			Fast switching with green	Address setting mode; RS 485 testing
		Green		ID media reading
	Right LED	Yellow	Continuously lit, flashing	Programming mode / PIN changing mode
			Short flashing with 1s per.	Indicating door lock release (optional)
		Green		Indicating door lock release

Table 7: LED indicators

4.4 Installation instructions

The reader module uses passive RF/ID technology, which is sensitive to RF noise sources. Noise sources are generally of two types: radiating or conducting.

Conducted noise enters the reader via wires from the power supply or the host. Sometimes, switching power supplies generate enough noise to cause reader malfunction, it is recommended to use linear system power supplies.

Radiated noise is transmitted through the air. It can be caused by computer monitors or other electrical equipment generating electromagnetic fields.

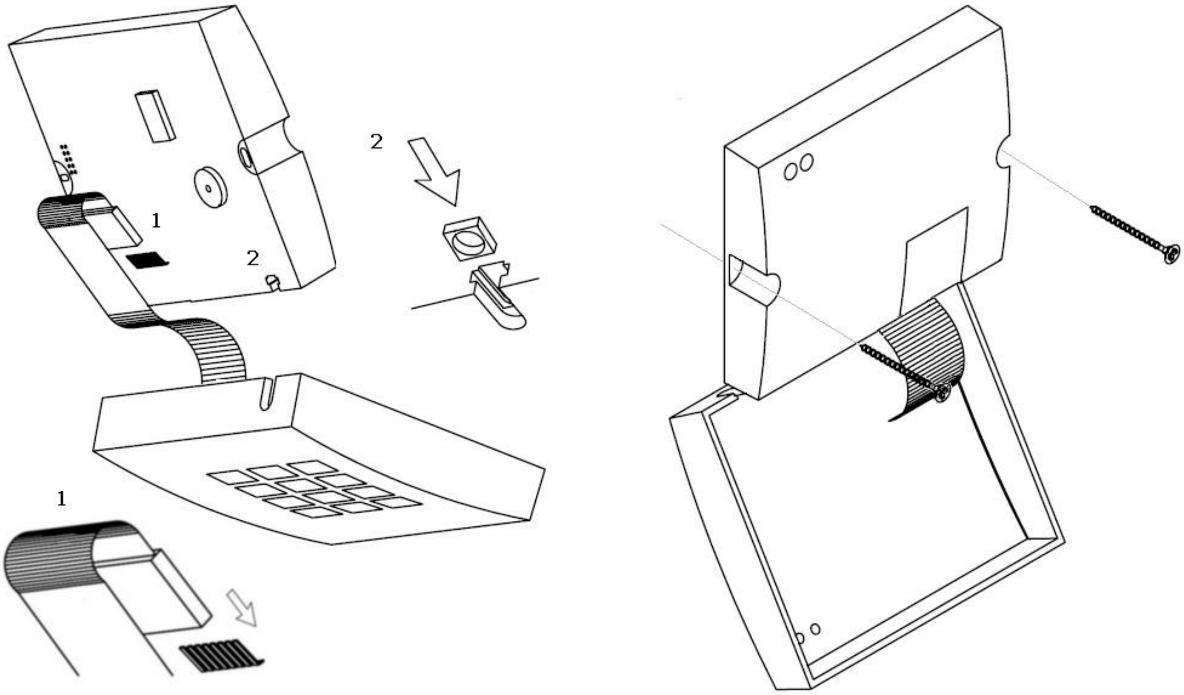
Consequently, a short distance between the reader modules themselves can cause reading malfunctions – for correct operation it is necessary to keep a minimum distance of 50 cm. Various metallic constructions may have a negative influence on this distance; if there are any doubts, it is recommended to make a practical test before final mounting.

Nearby metal surfaces may cause a decrease in reading distance and speed. This is caused by the combined effects of parasitic capacitance and conductance.

4.5 Mounting and removal the module

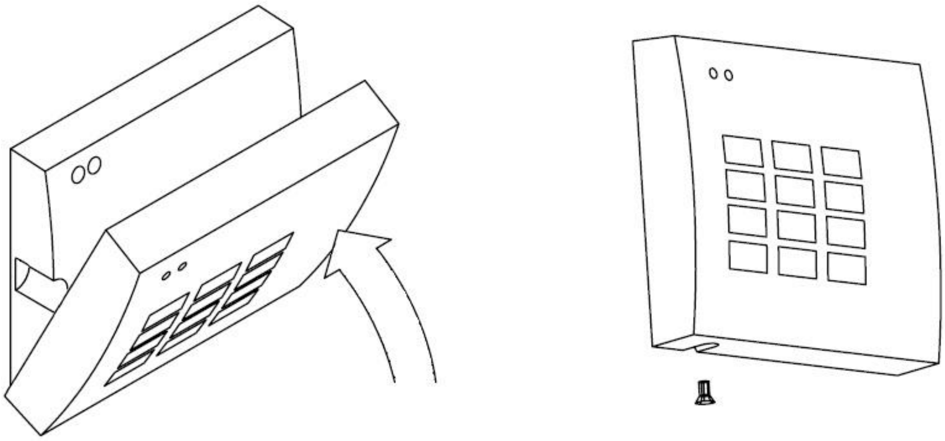
First drill the fastening and cable holes, then insert the flat keypad cable into the reader connector 1 carefully (when it is a keypad version), insert the enclosed square screw nut 2 and fasten the module on the wall, see *Pic. 4 a)*.

It is recommended to place an installation box for connection of incoming cables on the other side of the wall or in highly secured area (with in/out readers).



Pic. 4 a): Fastening the module on the wall

Shut the cover and lock it using enclosed screw, see *Pic. 4 b)*.



Pic. 4 b): Swinging on and locking the cover

Removal of the module can be performed in reverse order.

5 Setting parameters of the reader module

5.1 *Configurable parameters*

	Parameter		Possible range	Default setting
Configurable parameters	Door lock release time		0 ÷ 255 s	7 s
	Door lock control setting		Direct / reverse	Direct
	Door lock relay function setting		Standard / toggle / pulse	Standard
	Permanent door lock release according to a time schedule		Never / Schedule index	Never
	Door lock status indication		YES / NO	NO
	Acoustic signal of door lock release		YES / NO	YES
	Door ajar time		0 ÷ 255 s	20 s
	First input configuration		Door contact / REX button	Door contact
	Second input configuration		REX button / handle contact / tamper / disabling function	REX button
	Third input / output port		Tamper / ext. buzzer signal / IDS status monitoring / disabling function / reading synchronization	Tamper
	Acoustic signalization time - Tamper		0 ÷ 255 s	30 s
	Acoustic signalization time - Forced door		0 ÷ 255 s	30 s
	Acoustic signalization time – Door ajar		0 ÷ 255 s	0 s
	Acoustic signalization time – APB alarm		0 ÷ 255 s	0 s
	Signalization time – Card alarm		0 ÷ 255 s	30 s
	Antipassback function setting		See *chapter 6.10*	Disabled
	Automatic summer time adjustment		YES / NO	YES
	Release lock with REX button while tamper alarm active		YES / NO	YES
	Online authorization timeout		0 ÷ 25500 ms	800 ms
	Standalone authorization after timeout		YES / NO	YES
	Saving events in the module’s archive	Door opened	Enabled / Disabled	Enabled
		Door closed	Enabled / Disabled	Enabled
		Input 2 On	Enabled / Disabled	Enabled
		Input 2 Off	Enabled / Disabled	Enabled
		Strike released	Enabled / Disabled	Enabled
		Strike closed	Enabled / Disabled	Enabled

Table 8: Configurable parameters

5.2 *Reader module parameters setting*

Detailed instructions for setting reader module parameters are described in the *APS Reader* configuration program user’s guide available at the address http://www.techfass.cz/files/m_aps_miniplus_reader_en.pdf.

6 Reader module functioning

The reader module supports the following functions:

- Standard “Door Open” function.
- Door status monitoring.
- Exit-devices contact monitoring.
- Alarm output activated / acoustic signalization activated when any alarm condition occurs.

The “Door Open” function can be activated in 3 different ways:

- Reading a valid ID (card, key fob…).
- Pressing the exit button (according to configuration) – cannot be used in alarm condition.
- Via communication line (program request).

6.1 “Door Open” function description

In case the *standard function of the door lock relay* is set, the door lock is *released* and the *beeper activated* (when not disabled) when the “Door Open“ function is activated. Both outputs stay active until the door is opened or the preset door lock release time has elapsed - see *configuration table*.

In case the *toggle function of the door lock relay* is set, the door lock relay status is *switched* and the *beeper* is *activated* (when not disabled) when the “Door Open” function is activated. The beeper stays active until the door is opened or the preset door lock release time has elapsed - see *configuration table*. The door lock relay status remains unchanged until another “Door Open” function is activated.

In case the *pulse function of the door lock relay* is set, the door lock relay status is switched for the time defined by the *Pulse width* parameter (*ms*) after the Door Open function is activated.

In case the standard function of the door lock relay is set, reading a valid card during door lock release resets the door lock release time.

6.2 Function permanent door lock release according to a time schedule

When the function is set, the door lock is permanently released when relevant time schedule is valid. Reading a valid ID is standardly announced via the communication line (in online operating mode). The forced door alarm cannot be raised when the door lock is permanently released.

The permanent door lock release function and the toggle function of the door lock relay are mutually exclusive.

6.3 Alarm states

The reader module can get in following alarm states:

1) Tamper alarm
2) Forced door alarm
3) Door ajar alarm
4) Antipassback alarm (Time APB alarm, Zone APB alarm)
5) ID with Alarm flag alarm, Duress PIN alarm

Alarm state reporting is performed as follows:

- Via communication line (statuses 1, 2, 3, 4, 5)
- By acoustic signal (beeper) (statuses 1, 2, 3, 4).
- Activating the alarm output (AUX output) (statuses 1, 2, 3, 5).

Alarm signaling via communication line requires online running PC with relevant software suitable for online operation (APS 400 nAdministrator).

Two ways of acoustic signaling is carried out:

- Steady signal (tamper).
- Intermittent signal (forced door and/or door ajar, APB alarm).

Acoustic alarm signaling is stopped after a valid ID is presented or pre-set time interval is elapsed, see the configuration table.

If any of the relevant alarm states *(with setting of the signaling timer > 0)* occurs, the alarm output is activated. It can control any alarm device directly or it can be processed further.

After terminating all alarm conditions the alarm output is deactivated.

The alarm signaling is triggered by any alarm condition.

6.3.1 Tamper alarm

In case of tampering the module (by tearing-off (requires MAG) or changing the status of input 2 or input 3 in proper configuration) the “Tamper” state is activated [3)].

[3)] The Tamper alarm handling is operational after their first change of status since switching on the module. There is no need to configure the module when the tamper protection is not used.

6.3.2 Forced Door alarm

The “Forced Door” alarm state is activated when the door is opened without activating the “Door Open” function. The only exception is opening the door with the second module input IN2 active and configured as a handle contact.

6.3.3 Door Ajar alarm

If the door stays open until the pre-defined Door ajar timeout expires – see *Tab. 12*, the “Door Ajar“ alarm is activated.

6.3.4 Antipassback alarm

The *Antipassback alarm* is raised when an ID is read during the *Time APB* counter is running or when the ID is blocked by a *Zone APB*.

6.3.5 ID with Alarm flag alarm, Duress PIN alarm

ID with Alarm flag alarm occurs when an ID with the Alarm flag is read. *Duress PIN alarm* occurs when a user uses *duress PIN code* for identification.

6.3.6 Reading ID during alarm state

Reading an ID doesn't affect the alarm state, reading a valid ID only terminates the acoustic alarm announcement followed by "Door Open" function. Reading an invalid ID only interrupts the acoustic announcement of the alarm state while signalizing "Invalid ID".

6.4 Standard operating modes

The reader module can be in either *online* or *offline* operating mode. The module's functionality is identical in both operating modes; the events archive is read from the reader module's memory when the module goes online. When a programming card is read (while in either online or offline mode), the module goes into programming mode.

6.5 Read ID media format

6.5.1 EM Marin ID media format

The EM Marin ID media format can be changed into selected 24, 32 or 40 bits length of ID code. The default length is 40 bits. This setting is only used when unifying of the ID media codes length is required – in combined systems with WIEGAND output readers with a fixed WIEGAND data format IDs (more information in *APS Reader* user's guide available at http://www.techfass.cz/files/m_aps_miniplus_reader_en.pdf).

6.6 Wiegand interface configuration

6.6.1 Standard operating mode

This is the module default operating mode. The Wiegand interface is used for controlling the WIO 22 module in this configuration. When the reader module operates in the standard operating mode, the I/O Port (*tab. 5*) is used as an input for monitoring an external device tamper status.

6.6.2 Wiegand output

The module can be configured into a standard reader with a *WIEGAND output* in 26, 32, 42 or 44 bits format for *EM Marin* technology ID media. Read IDs are formatted with the previous setting first (see *chapter 6.5.1*), after that they are sent in the output format. When the reader module operates in the Wiegand output operating mode, the I/O Port (*tab. 5*) is used as an input for monitoring an external device tamper status.

Wiegand	ID media technology	Available configuration of the WIEGAND output format
	EM Marin	26bit, 32bit, 42bit, 44bit

Table 9: ID media format in WIEGAND operating mode

Two long beeps and the red LED lit feature powering up the module. The green LED blink indicates an ID reading.

Individual signals function in *WIEGAND output* operating mode is described in *table 10*.

Wiegand	Input 1	Beeper control (0 V active)
	Input 2	Yellow LED control (0 V active)
	Output 1 (relay)	Tamper signaling; it follows the alarm state of tamper sensors (tamper signal = relay switched on) [3]

Table 10: Signal function in WIEGAND operating mode

Key codes sent in *WIEGAND output* operating mode are described in *table 11*.

Pressed key interpretation	Keypad version	Pressed key	Keypad function set in program	
			PIN / ID keypad function	Key code keypad function
	MREP 73	Keys 1 ÷ 9	Code 1 ÷ 9	
		Keys 0	Code 0	Code 10
		X (ESC)	Code 10	Code 0
		↲ (ENTER)	Code 11	
		↑ (up arrow)	Code 12	
		↓ (down arrow)	Code 13	
		→ (right arrow)	Code 14	
		← (left arrow)	Code 15	
	MRED 73	Keys 1 ÷ 9	Code 1 ÷ 9	
		Keys 10	Code 0	Code 10
		ESC	Code 10	Code 0
		ENTER	Code 11	
		F1	Code 12	
		F2	Code 13	
		F3	Code 14	
		F4	Code 15	

Table 11: Pressed key interpretation in WIEGAND output mode

Since the *FW version 5.09* the reading synchronization of a *couple of TECHFASS readers* is implemented, enabling to *cancel the mutual disturbance* of the modules. The reader module offers the *Wiegand data interface synchronization* in *MASTER* mode.

6.6.3 Wiegand input (entry reader)

The module can be configured into a mode of controlling the door from both sides (*entry reader mode*).

In the *entry reader mode* an identification at an external reader connected via the *WIEGAND interface* acquires a *reason code 255*; at the same time the reader module operates standardly, the reason codes equal zero.

When the reader module operates in the entry reader operating mode, the I/O Port (*tab. 5*) is used as an output for controlling the entry reader buzzer.

Since the *FW version 5.09* the reading synchronization of a *couple of TECHFASS readers* is implemented, enabling to *cancel the mutual disturbance* of the modules. The reader module offers the *Wiegand data interface synchronization* in *SLAVE* mode.

The *WIEGAND input* and *WIEGAND output* operating modes are mutually exclusive.

6.7 Keypad function

The keypad function setting can be set to one of the following options:

- *Key code* – this option is used when the keypad is used for entering a code of reason to exit.
- *PIN* – with this option selected the keypad is used for entering PIN codes, a correct PIN is required for valid identification when this option is selected

If the "*Suppress PIN request according to a time schedule*" function is set, the PIN code entering is not requested when the used time schedule is valid.

- *ID* – this option enables entering a code at the keypad which is used as a user's read ID medium; the time for locking up the keypad when an unknown ID is entered 5 times in a row can be set there as well, the setting range is from 0 to 2550s with a 10s step.

Table 12 defines the interpretation of keys pressed at the individual keypads design of *MREx 73 reader modules* according to the program configuration of the keypad function.

Pressed key interpretation	Keypad version	Pressed key	Keypad function set in program	
			PIN / ID keypad function	Key code keypad function
	MREP 73	Keys 1 ÷ 9	Digits 1 ÷ 9	Reason 1 ÷ 9
		Keys 0	Digit 0	Reason 10
		X (ESC)	Digits input cancel, reason 0	Reason 0
		↲ (ENTER)	Input submit	Reason 11
		↑ (up arrow)	Reason 12	Reason 12
		↓ (down arrow)	Reason 13	Reason 13
		→ (right arrow)	Reason 14	Reason 14
		← (left arrow)	Reason 15	Reason 15
	MRED 73	Keys 1 ÷ 9	Digits 1 ÷ 9	Reason 1 ÷ 9
		Keys 10	Digit 0	Reason 10
		ESC	Digits input cancel, reason 0	Reason 0
		ENTER	Input submit	Reason 11
		F1	Reason 12	Reason 12
		F2	Reason 13	Reason 13
		F3	Reason 14	Reason 14
		F4	Reason 15	Reason 15

Table 12: Pressed key interpretation

Note: When the operating mode "*Standard with IDS control*" is set, the press of *ENTER* key *before identification start* is interpreted as *request for changing the armed/disarmed status of the IDS*.

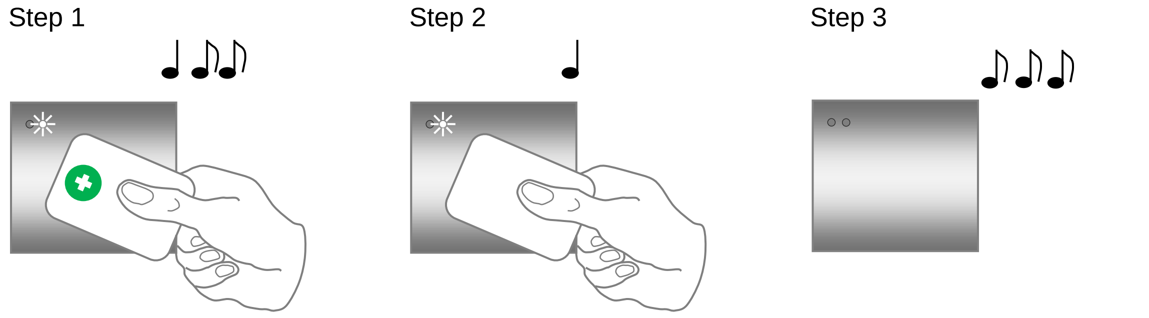
6.8 Programming mode

The module enters programming mode by reading one of the two *programming cards* (cards "+" and "-"). The programming mode cannot be entered while the module is in hardware address setting mode (for modules with HW address setting via the communication line). The module's functionality in programming mode can be seen in *pictures 5 a-d*.

It is not possible to use time schedules when inserting cards in programming mode, therefore cards are always valid. Any user inserted using a programming card has a default PIN set to *12345*.
If the reader module's keypad is set as a code keypad, the programming mode can be entered by entering the right code at the keypad. It is also possible to insert cards using a keypad on modules with a code keypad.

6.8.1 Inserting cards (codes) into the reader's memory

Follow these steps for inserting cards into the reader module's memory:



Step 1

Read the programming card (or enter the programming code) for *inserting*: the reader goes into *programming mode*.

Step 2

One by one, read the cards (enter user codes) which are to be granted access.

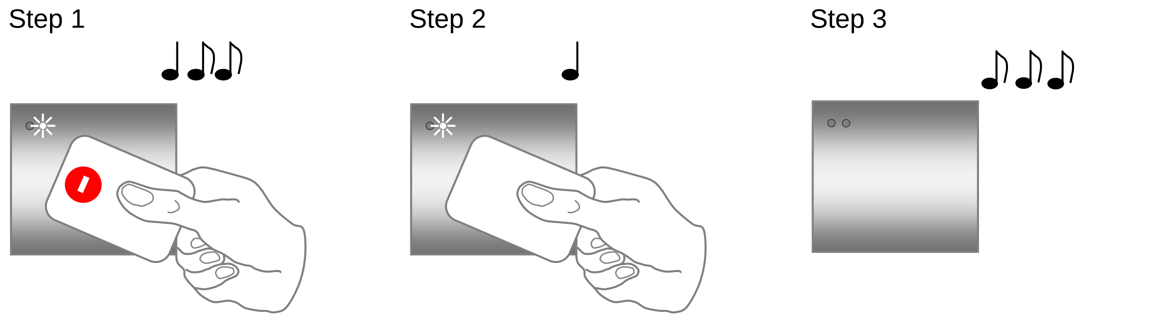
Step 3

About 15 seconds after inserting the last card (code) the reader module goes back into *standard operating mode*.

Pic.5 a): Inserting cards (codes)

6.8.2 Deleting cards (codes) from the reader's memory

For deleting the cards from the reader module's memory use following steps:



Step 1

Read the programming card (or enter the programming code) for *deleting*: the reader goes into *programming mode*.

Step 2

One by one, read the cards (enter user codes) which are to have their access revoked.

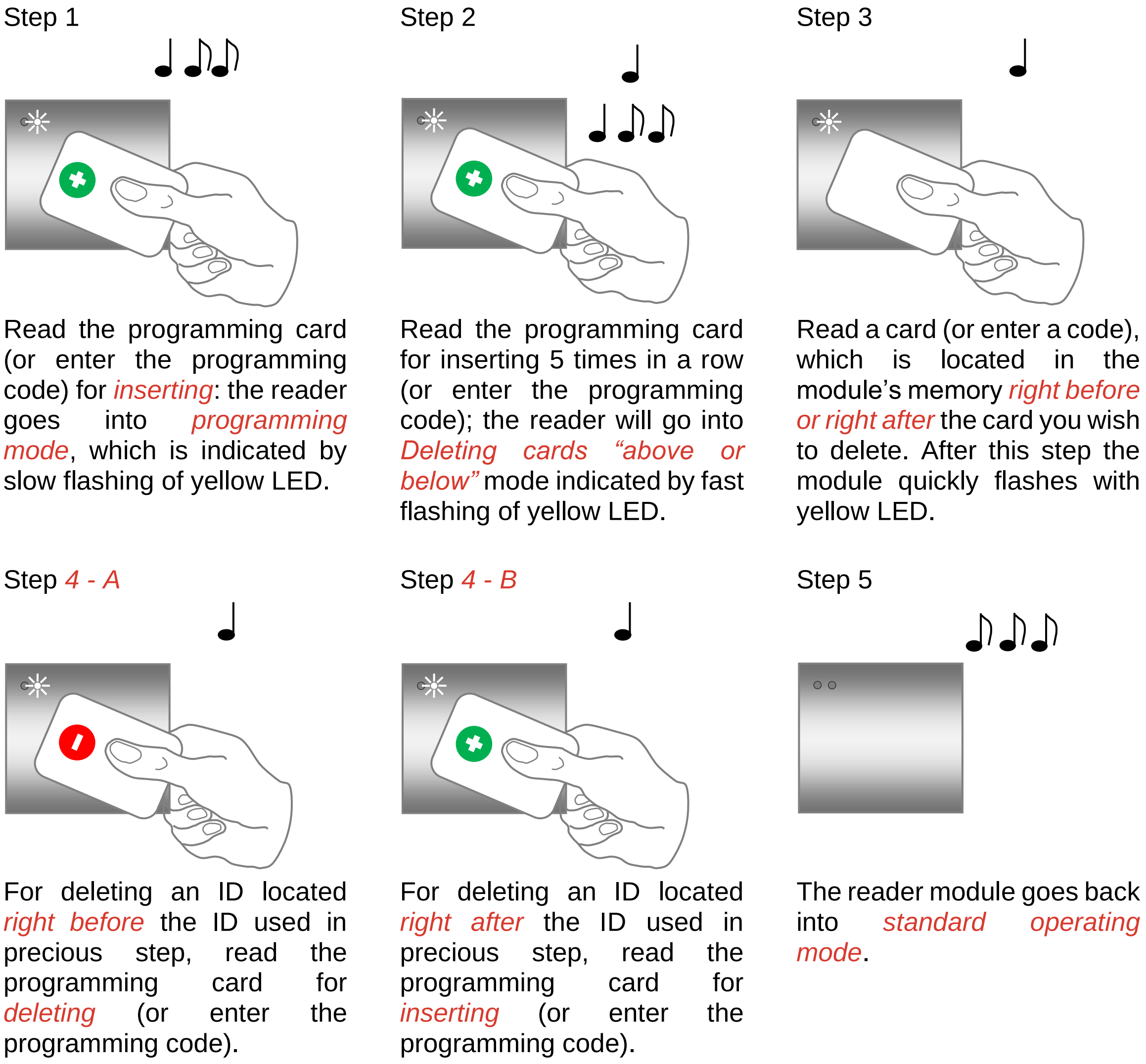
Step 3

About 15 seconds after deleting the last card (code) the reader module goes back into *standard operating mode*.

Pic.5 b): Deleting cards (codes)

6.8.3 Deleting cards (codes) „above or below“

If a user loses his ID medium, it is usually impossible to delete the ID from the memory with the procedure described in the previous chapter, since the medium is no longer available (with an exception of entering the code at the keypad). Following procedure can be used for deleting such ID. The procedure *requires using an ID medium*, which was inserted *right before or right after the ID medium*, which should be deleted.



Step 1

Read the programming card (or enter the programming code) for *inserting*: the reader goes into *programming mode*, which is indicated by slow flashing of yellow LED.

Step 2

Read the programming card for inserting 5 times in a row (or enter the programming code); the reader will go into *Deleting cards "above or below"* mode indicated by fast flashing of yellow LED.

Step 3

Read a card (or enter a code), which is located in the module's memory *right before or right after* the card you wish to delete. After this step the module quickly flashes with yellow LED.

Step *4 - A*

For deleting an ID located *right before* the ID used in precious step, read the programming card for *deleting* (or enter the programming code).

Step *4 - B*

For deleting an ID located *right after* the ID used in precious step, read the programming card for *inserting* (or enter the programming code).

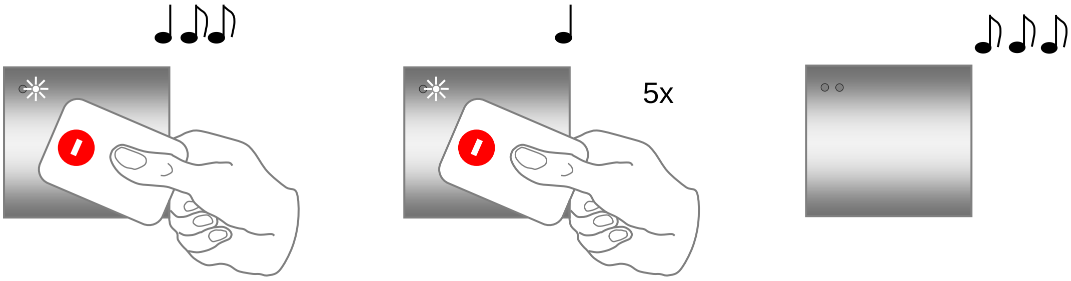
Step 5

The reader module goes back into *standard operating mode*.

Pic.5 c): Deleting cards (codes) "above or below"

6.8.4 Deleting all cards (codes) from the reader's memory

Follow these steps for deleting all cards from the reader module's memory:



Step 1

Read the programming card (or enter the programming code) for *deleting*: the reader goes into *programming mode*.

Step 2

Read the programming card for deleting 5 times in a row (or enter the programming code); the reader will erase all cards from its memory.

Step 3

The reader module goes back into *standard operating mode*.

Pic.5 d): Deleting all cards (codes)

6.8.5 Recommended method for access rights management (using prog. cards)

In case of managing access rights of plenty of users (using programming cards only), it is appropriate to establish a table, which summarizes operation with the reader module memory. All operations (adding and deleting cards) should be stored in the table. Following example shows correct usage of the programming cards and proper filing of the actions:

- Inserting *5 new cards* using the procedure from *chapter 6.8.1* – Read *+ (inserting) programming card*, read *cards 1-5*, after 15 s the programming mode is exited, *create a table*.

position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5

Pic.5 e): Table after inserting 5 cards

- *Card 3 gets lost* – Delete it *using the card 4*, which is available, and using the procedure from *chapter 6.8.3* – Read *+ (inserting) programming card*, then *5x + (inserting) programming card* again, then *card 4*, and finally *– (deleting) programming card*. *Register the change in your table*.

position	card
1	card 1
2	card 2
3	card 3 (lost)
4	card 4 (available)
5	card 5

position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5

Pic.5 f): Deleting card 3 using the card 4, table after deleting card 3

- *Card 4 gets lost* – Delete it *using the card 2*, which is available, and using the procedure from *chapter 6.8.3* – Read *+ (inserting) programming card*, then *5x + (inserting) programming card* again, then *card 2*, and finally *+ (inserting) programming card* again. *Register the change in your table*.

position	card
1	card 1
2	card 2 (available)
3	card 3
4	card 4 (lost)
5	card 5

→

position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5

Pic.5 g): Deleting card 4 using the card 2, table after deleting card 4

- It is necessary to *add another card* (card 6). We proceed with the procedure from *chapter 6.8.1* again. *1* – Read *+ (inserting) programming card*, read *cards 1-5*, after 15 s the programming mode is exited. *Register the change in your table*.

position	card
1	card 1
2	card 2
3	card 3
4	card 4
5	card 5
6	card 6

Pic. 5 h): Table after inserting card 6

A new card is always inserted at the position after the last inserted card. In case of deleting all cards using the procedure described in *chapter 6.8.4*, it is necessary to create a new filing table.

6.8.6 PIN change

It is possible to change a PIN code in the reader's memory by pressing the key sequence *Esc - 1 – Enter* (at a reader in a mode with a keypad for PIN entering). The reader enters *PIN changing mode*. In this mode the user attempting to change his PIN code must first validate *his identity by reading his ID* card and entering the *current PIN code*; then he enters the *new PIN*, *Enter* key, *new PIN again* and finally *Enter* key again. A record is stored in the events archive whenever a PIN code is changed by a user (if the events archive is available).

6.9 ID expiration function

This function is implemented since the FW version 5.0.

It is possible to set an *Expiration date* for every *ID* stored in the module. When the date occurs, the ID becomes invalid (expired). The expiration evaluation is performed on every date change in the module's RTC and when the access rights are downloaded.

6.10 ID with Alarm flag function

This function is implemented since the FW version 5.0.

It is possible so set an *Alarm – ID flag* for every *ID* stored in the module. When the ID is read, relevant alarm is raised (and the alarm output is switched for preset time).

6.11 Antipassback function

This function is implemented since the FW version 5.0.

The Antipassback function is defined in two ways:

- *Time APB* – user cannot repeatedly use his ID for defined time
- *Zone APB* – user cannot repeatedly enter an area, where he is already present

The Antipassback function is used *only for the users*, whose access is driven by a *time schedule*. The users with access always granted are not affected by the Antipassback function.

The Antipassback flags for an *ID* can be *reset* by *inserting the ID again* with use of the *programming cards* (offline solution). *All Antipassback flags* are also *reset* whenever new *access rights data are downloaded* from the program.

Both Zone and Time Antipassback flags are written either immediately *after an ID is read*, or after relevant *door is opened* (relevant input is disconnected).

6.11.1 Time Antipassback

The *Time Antipassback* is defined by the *ABP timer initial value* (in minutes), which is set to the ID after passing at the reader module. If the users uses the ID at the address during the timer for the ID is running, the Time APB alarm is raised. Following parameters affect the Time APB function:

- *APB timer initial value* – defines the Time APB flag (timer) value set to the ID after passing at the reader module. If a user uses the ID again before the timer elapses, Time APB alarm is raised.
- *Open door after APB time alarm* – if the option is enabled, the Door open function is performed after the Time APB alarm is raised.

6.11.2 Zone Antipassback

The *Zone Antipassback* is defined by *enabling the option* for the relevant address. The Zone APB flag is set for the ID when passing at the reader module. If a user uses the ID again when the Zone APB flag is set, the Zone APB alarm is raised. Following parameters affect the Zone APB function:

- *Enabled* – enable/disable general Zone APB flag setting.
- *Enable in offline mode* – if the option is not set, the module operates in offline mode like if the APB function was not implemented.
- *Open door after APB Zone alarm* – if the option is enabled, the Door open function is performed after the Zone APB alarm is raised.

6.12 Duress PIN

This function is implemented since the FW version 5.2.

To use the *Duress PIN* code entering function, use the user's standard PIN code with the last digit increased by 1. If the last digit equals 9, it is changed to 0 when using this function.

6.13 Disabling function

This function is implemented since the *FW version 5.08*.

The *module disabling function* can be set at the second input and at the third input / output port. The logic of the function is individually configurable. The function is active whenever one or both of the configured inputs are active.

The module behavior is as described below when the disabling function is active:

- User with access driven by a time schedule cannot run the door open function
- User with access always granted is not affected by the disabling function
- Remote door open function cannot be performed
- Remote identification with ID is disabled for users with access driven by a time schedule

The disabling status changes and disabled actions are logged in the events archive.

6.14 Reading synchronization

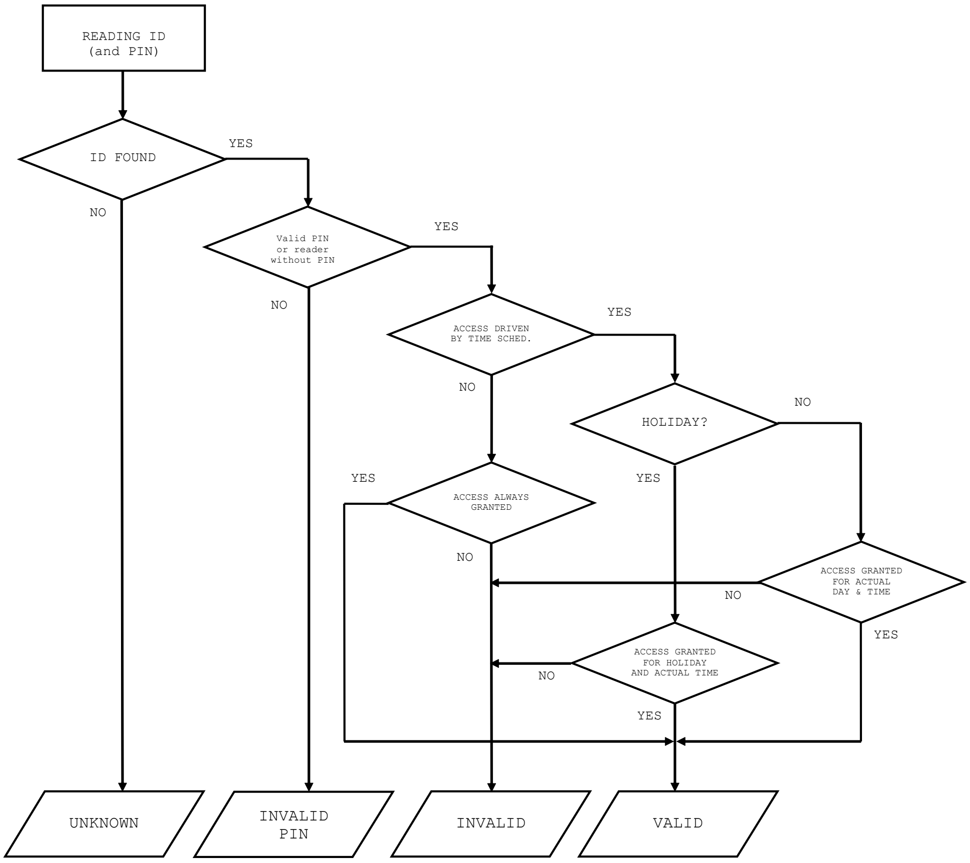
Since the *FW version 5.09* the reading synchronization of a *couple of TECHFASS readers* is implemented, enabling to *cancel the mutual disturbance* of the modules. The reader module offers to use the *IO synchronization* in both *MASTER* and *SLAVE* mode. The *input/output port 3* is used as the *synchronization signal*.

6.15 Online authorization

Since the *FW version 5.11* the *Online authorization of ID* can be used in APS mini Plus system. When the feature is used, the ID validity is resolved in connected PC. To be able to use this authorization mode, the reader module has to be equipped with a *MLO* license.

7 Simplified access rights evaluation

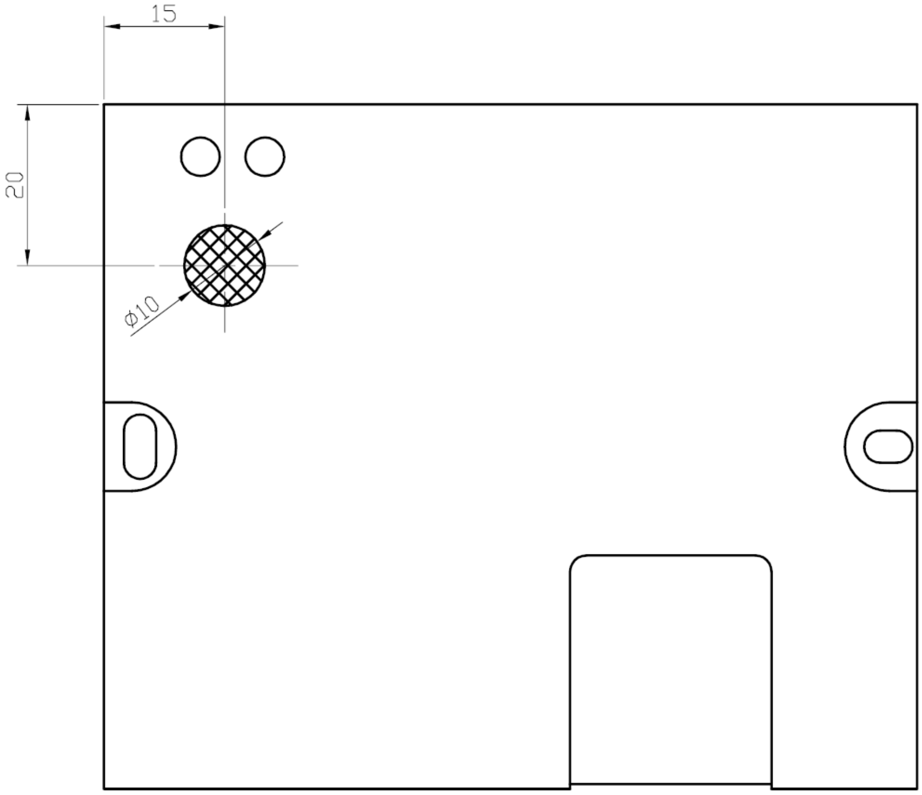
The model of access rights contains time schedules and a table of holidays. A block diagram for access right evaluation can be seen on *Pic.6.*



Pic. 6: Simplified access rights evaluation

8 Placing a magnet for tearing-off indication

Drill a ∅ 10 mm hole 12 mm deep in a wall behind the reader module at designated place (*Pic. 7*). Insert a magnet (ordering number 51900200) and attach it in the hole with appropriate mastic to ensure the top surface of the magnet matches with the wall surface. Mount the reader module in formerly prepared holes mounted with plugs.



Pic. 7: Placing magnet for tearing-off indication

9 Useful links

- Wiring diagrams: http://techfass.cz/diagrams-aps-mini-plus-en.html
- Program equipment: http://techfass.cz/software-and-documentation-en.html